Appendix D-1

Communication Log

Day 2			
From	**Time Sent**	**Received**	**Contents of Message**
Mobile Unit	L5 4/13/99 4:35:13 PM	Tue 4/13/99 4:36 PM	14GCE6643TA021548
Mobile Unit	L5 4/12/99 9:08:03 PM	Mon 4/12/99 9:09 PM	14GCE6643TA021548
Mobile Unit	L5 4/12/99 3:22:06 PM	Mon 4/12/99 3:23 PM	14GCE6643TA021548
Mobile Unit	L5 4/12/99 3:19:40 PM	Mon 4/12/99 3:20 PM	14GCE6643TA021548
Mobile Unit	L5 4/12/99 3:17:08 PM	Mon 4/12/99 3:18 PM	14GCE6643TA021548
Mobile Unit	L4 4/12/99 3:15:43 PM	Mon 4/12/99 3:17 PM	1P3EJ46C1WN195873
Mobile Unit	L5 4/12/99 3:15:04 PM	Mon 4/12/99 3:16 PM	14GCE6643TA021548
Mobile Unit	L5 4/12/99 3:12:37 PM	Mon 4/12/99 3:13 PM	14GCE6643TA021548
Mobile Unit	L5 4/12/99 3:09:47 PM	Mon 4/12/99 3:11 PM	14GCE6643TA021548

Day 3			
From	**Time Sent**	**Received**	**Contents of Message**
ardisce007	L2 4/14/99 7:53:12 AM	Wed 4/14/99 11:14 AM	1MEFM50U3WG625151 F:P0155 O2 HEATER CKT BANK #2, SNSR #1 F:P1151 UNDOCUMENTED CODE
ardisce007	L2 4/14/99 7:53:12 AM	Wed 4/14/99 11:13 AM	1MEFM50U3WG625151 F:P0155 O2 HEATER CKT BANK #2, SNSR #1 F:P1151 UNDOCUMENTED CODE
ardisce007	L2 4/14/99 7:53:12 AM	Wed 4/14/99 11:12 AM	1MEFM50U3WG625151 F:P0155 O2 HEATER CKT BANK #2, SNSR #1 F:P1151 UNDOCUMENTED CODE
ardisce007	L2 4/13/99 6:15:37 PM	Wed 4/14/99 11:11 AM	1MEFM50U3WG625151 F:P1151 UNDOCUMENTED CODE
Mobile Unit	L5 4/14/99 8:58:20 AM	Wed 4/14/99 8:59 AM	14GCE6643TA021548 F:P0122 THROTTLE POSITION CIRCUIT SHORT F:P1790 UNDOCUMENTED CODE
Mobile Unit	L5 4/14/99 8:21:07 AM	Wed 4/14/99 8:22 AM	14GCE6643TA021548 F:P0122 THROTTLE POSITION CIRCUIT SHORT F:P1790 UNDOCUMENTED CODE
Mobile Unit	L4 4/13/99 5:48:44 PM	Tue 4/13/99 5:50 PM	1P3EJ46C1WN195873 F:P0403 EGR SOLENOID CIRCUIT PROBLEM
Mobile Unit	L3 4/13/99 5:39:35 PM	Tue 4/13/99 5:40 PM	2G1WL52M3W9243369 F:P0122 THROTTLE POSITION CIRCUIT SHORT

Day 4			
From	**Time Sent**	**Received**	**Contents of Message**
Mobile Unit	L5 4/14/99 8:49:54 PM	Wed 4/14/99 8:50 PM	14GCE6643TA021548
ardisce007	L2 4/14/99 6:07:24 PM	Wed 4/14/99 6:07 PM	1MEFM50U3WG625151 F:P0102 AIRFLOW SIGNAL VOLTAGE LOW
Mobile Unit	L4 4/14/99 5:45:32 PM	Wed 4/14/99 5:47 PM	1P3EJ46C1WN195873 F:P0108 MAP/BARO CIRCUIT VALUE HIGH F:P0113 INTAKE AIR TEMP VALUE HIGH
Chitiger 11	L1 4/14/99 5:45:06 PM	Wed 4/14/99 5:46 PM	YV1KS9604V1116649 F:P0102 AIRFLOW SIGNAL VOLTAGE LOW
Mobile Unit	L5 4/14/99 4:14:38 PM	Wed 4/14/99 4:15 PM	14GCE6643TA021548
Mobile Unit	L5 4/14/99 4:01:22 PM	Wed 4/14/99 4:02 PM	14GCE6643TA021548
Mobile Unit	L5 4/14/99 3:38:03 PM	Wed 4/14/99 3:55 PM	14GCE6643TA021548
Mobile Unit	L5 4/14/99 3:38:03 PM	Wed 4/14/99 3:55 PM	14GCE6643TA021548
Mobile Unit	L4 4/14/99 12:03:18 PM	Wed 4/14/99 12:05 PM	1P3EJ46C1WN195873 F:P0113 INTAKE AIR TEMP VALUE HIGH
Mobile Unit	L5 4/14/99 11:30:32 AM	Wed 4/14/99 12:05 PM	14GCE6643TA021548

Day 5			
From	**Time Sent**	**Received**	**Contents of Message**
Mobile Unit	L1 4/16/99 11:31:23 AM	Fri 4/16/99 3:18 PM	YV1KS9604V1116649 F:P0120 THROTTLE POSITION SENSOR F:P0123 THROTTLE POSITION CIRCUIT OPEN
Mobile Unit	L3 4/15/99 5:40:13 PM	Fri 4/16/99 11:53 AM	2G1WL52M3W9243369 F:P0102 AIRFLOW SIGNAL VOLTAGE LOW F:P0122 THROTTLE POSITION CIRCUIT SHORT
Mobile Unit	L3 4/16/99 7:36:15 AM	Fri 4/16/99 11:39 AM	2G1WL52M3W9243369 F:P0102 AIRFLOW SIGNAL VOLTAGE LOW F:P0122 THROTTLE POSITION CIRCUIT SHORT
Mobile Unit	L3 4/16/99 11:20:46 AM	Fri 4/16/99 11:39 AM	2G1WL52M3W9243369 F:P0102 AIRFLOW SIGNAL VOLTAGE LOW F:P0122 THROTTLE POSITION CIRCUIT SHORT
Mobile Unit	L3 4/13/99 5:39:35 PM	Fri 4/16/99 11:39 AM	2G1WL52M3W9243369 F:P0122 THROTTLE POSITION CIRCUIT SHORT
Mobile Unit	L3 4/16/99 11:28:02 AM	Fri 4/16/99 11:29 AM	2G1WL52M3W9243369 F:P0102 AIRFLOW SIGNAL VOLTAGE LOW F:P0122 THROTTLE POSITION CIRCUIT SHORT
Chitiger 11	L1 4/16/99 11:22:05 AM	Fri 4/16/99 11:23 AM	YV1KS9604V1116649 F:P0120 THROTTLE POSITION SENSOR F:P0123 THROTTLE POSITION CIRCUIT OPEN
Mobile Unit	L5 4/16/99 11:21:14 AM	Fri 4/16/99 11:22 AM	14GCE6643TA021548 F:P0441 EVAP SYSTEM PURGE FLOW LOW
ardisce007	L2 4/16/99 11:21:42 AM	Fri 4/16/99 11:21 AM	1MEFM50U3WG625151 F:P0122 THROTTLE POSITION CIRCUIT SHORT
Mobile Unit	L5 4/16/99 8:55:35 AM	Fri 4/16/99 8:56 AM	14GCE6643TA021548 F:P0441 EVAP SYSTEM PURGE FLOW LOW
Mobile Unit	L4 4/16/99 7:41:37 AM	Fri 4/16/99 7:43 AM	1P3EJ46C1WN195873
Chitiger 11	L1 4/16/99 7:04:38 AM	Fri 4/16/99 7:30 AM	YV1KS9604V1116649 F:P0120 THROTTLE POSITION SENSOR F:P0123 THROTTLE POSITION CIRCUIT OPEN
ardisce007	L2 4/15/99 6:10:25 PM	Thu 4/15/99 6:18 PM	1MEFM50U3WG625151 F:P0122 THROTTLE POSITION CIRCUIT SHORT

Day 5			
From	**Time Sent**	**Received**	**Contents of Message**
Mobile Unit	L5 4/15/99 6:01:50 PM	Thu 4/15/99 6:02 PM	14GCE6643TA021548 F:P0441 EVAP SYSTEM PURGE FLOW LOW
Mobile Unit	L4 4/15/99 6:00:26 PM	Thu 4/15/99 6:02 PM	1P3EJ46C1WN195873
ardisce007	L2 4/15/99 5:57:06 PM	Thu 4/15/99 5:57 PM	1MEFM50U3WG625151 F:P0122 THROTTLE POSITION CIRCUIT SHORT
Chitiger 11	L1 4/15/99 5:54:27 PM	Thu 4/15/99 5:55 PM	YV1KS9604V1116649 F:P0120 THROTTLE POSITION SENSOR F:P0123 THROTTLE POSITION CIRCUIT OPEN
Chitiger 11	L1 4/15/99 5:48:02 PM	Thu 4/15/99 5:48 PM	YV1KS9604V1116649 F:P0123 THROTTLE POSITION CIRCUIT OPEN
ardisce007	L2 4/15/99 5:39:10 PM	Thu 4/15/99 5:39 PM	1MEFM50U3WG625151
Mobile Unit	L5 4/15/99 2:11:48 PM	Thu 4/15/99 2:13 PM	14GCE6643TA021548 F:P0441 EVAP SYSTEM PURGE FLOW LOW
Mobile Unit	L5 4/15/99 2:09:17 PM	Thu 4/15/99 2:10 PM	14GCE6643TA021548 F:P0441 EVAP SYSTEM PURGE FLOW LOW
Mobile Unit	L5 4/15/99 8:29:44 AM	Thu 4/15/99 8:31 AM	14GCE6643TA021548

Appendix D-2

ARB Mechanic's Maintenance Log

		Mechanic's OBDIII Vehicle Service Log							Page: 1	
Vehicle:	Volvo									
Mechanic Initials	Type of disablmnt	Date disablmnt installed	Time disablmnt installed	Date disablmnt removed	Time disablmnt removed	Date fault code(s) read	Time fault code(s) read	Fault codes (if any)	Date fault code(s) cleared	Time fault code(s) cleared
TA.	MAF	4/14/99	11:47am	4/15/99	2:55 pm	4/14/99	11:41 am	None	NA	
TH.	TPS	4/15/99	2:59 pm			4/15/99	2:55 pm	P0102 (MAF)	4/15/99	2:56 pm

		Mechanic's OBDIII Vehicle Service Log							Page: 1	
Vehicle:	Mercury - Sable (Ford)									
Mechanic Initials	Type of disablmnt	Date disablmnt installed	Time disablmnt installed	Date disablmnt removed	Time disablmnt removed	Date fault code(s) read	Time fault code(s) read	Fault codes (if any)	Date fault code(s) cleared	Time fault code(s) cleared
T.A.	O2 Sensor	4/13/99	5:06pm			4/13/99	5:02pm	None	N/A	
T.A.				4/14/99	12:12pm	4/14/99	12:08pm	P0155, P1151	4/14/99	12:11pm
T.A.	MAF	4/14/99	12:15pm							
T.A.				4/15/99	2:29pm	4/15/99	2:42pm	P0102 Airflow	4/15/99	2:43pm
T.A.	TPS	4/15/99	2:45pm							

		Mechanic's OBDIII Vehicle Service Log							Page: 1	
Vehicle:	Lumina									
Mechanic Initials	Type of disablmnt	Date disablmnt installed	Time disablmnt installed	Date disablmnt removed	Time disablmnt removed	Date fault code(s) read	Time fault code(s) read	Fault codes (if any)	Date fault code(s) cleared	Time fault code(s) cleared
T.A.	TPS	4/13/99	4:58 pm			4/13/99	4:51 pm	~~4:51 pm~~ None	N/A	N/A
TA				4/15/99	2:51 pm	4/15/99	2:46 pm	P0122 (TPS)	4/15/99	2:47 pm
T.A.	MAF	4/15/99	2:52 pm							

	plym.	Mechanic's OBDIII Vehicle Service Log							Page: 1	
Vehicle:	Breeze									
Mechanic Initials	Type of disablmnt	Date disablmnt installed	Time disablmnt installed	Date disablmnt removed	Time disablmnt removed	Date fault code(s) read	Time fault code(s) read	Fault codes (if any)	Date fault code(s) cleared	Time fault code(s) cleared
T.A.	EGR (VAC. VALVE)	4/13/99	5:13pm			4/13/99	5809 pm	None	N/A	
T.A.				4/14/99	11:53 Am	4/14/99	11:50 Am	P0403 EGR SOL. Faulty	4/14/99	11:53
T.A.	Charge air/ MAP	4/14/99	12:02pm			4/14/99	12:02 pm	P0113 Faulty	N/A	
T.A.				4/15/99	2:31pm	4/15/99	2:36	P0108, P0113 Map Bad \ Intake air temp.	4/15/99	2:38pm

		Mechanic's OBDIII Vehicle Service Log							Page: 1	
Vehicle:	ARB Honda									
Mechanic Initials	Type of disablmnt	Date disablmnt installed	Time disablmnt installed	Date disablmnt removed	Time disablmnt removed	Date fault code(s) read	Time fault code(s) read	Fault codes (if any)	Date fault code(s) cleared	Time fault code(s) cleared
T.A.	TBS	4/13/99	8:07pm			4/13/99	8:05pm	None	N/A	
T.A.				4/14/99	8:55Am	4/14/99	8:56am	P0122, P1790	4/14/99	8:57Am
HM	Evap & EGR	4/13/11	3:36 Am	4/14/99	8:55pm	4/14/99	8:55pm	TPS None Lundax.	N/A	
TA	EVAP Sol.	4/15/99	8:27Am			4/15/99	1:35pm	None		

Appendix D-3

Driver's Vehicle Usage Log

				Driver's OBDIII Vehicle Usage Log					Page:
Vehicle: Volvo									
Driver's Initials	Date	Time of engine start	Odometer at engine start	Location at engine start	CEL at engine start	Time of engine stop	Odometer at engine stop	Location at engine stop	CEL at engine stop
PT									
PT	4-12	18:07	25617	SR	off	18:36	25637	Home	off
	4-13	7:20	25637	Home	off	8:00	25659	Sierra	off
	4-13	10:25	25659	SR	off	11:05	25666	Fry's	off
	4-13	11:20	25666	Fry's	off	11:30	25673	Sierra	off
	4-13	19:00	25673	SR	off	19:24	25692	Home	off
	4-14	7:25	25692	Home	off	8:05	25715	SR	off
	4-14	17:45	25715	SR	on	18:22	25745	Home	on
	4-15	7:25	25745	Home	on	8:00	25766	SR	on
	4-15	9:20	25766	SR	on	9:30	25771	CompUSA	on
	4-15	10:25	25771	CompUSA	on	10:40	25776	SR	on
	4-15	17:50	25776	SR	on	18:15	25795	Home	on
	4-16	7:00	25795	Home	on	7:40	25817	SR	on

Driver's OBDIII Vehicle Usage Log

Page: 1

Vehicle: SABLE

Driver's Initials	Date	Time of engine start	Odometer at engine start	Location at engine start	CEL at engine start	Time of engine stop	Odometer at engine stop	Location at engine stop	CEL at engine stop	
FDG	4/12/99	18:11	31,039	SIERRA	OFF	18:33	31,054	DAVIS	OFF	
"	4/13/99	7:37	31,054	DAVIS	OFF	8:01	31,068	SIERRA	OFF	
"	4/13/99	17:51	31,068	SIERRA	OFF	18:02	31,073	W.SACTO(GAS)	OFF	
"	4/13/99	18:03	31,073	W.SACTO	OFF	18:04	31073	"	OFF	
"	4/13/99	18:10	31,073	W.SACTO	OFF	18:24	31083	DAVIS	ON	
"	4/14/99	7:38	31,083	DAVIS	ON	8:05	31,098	SIERRA	ON	
"	4/14/99	17:49	31,098	SIERRA	OFF	18:00	31,101	W.SACTO	OFF	
"	4/14/99	18:04	31,101	W.SACTO	OFF	18:21	31,113	DAVIS	ON	
"	4/15/99	7:44	31,113	DAVIS	ON	8:07	31,128	SIERRA	ON	
JM	4 15 99	17 34	31,128	Sierra	off	17 38	31129	25 V	off	
	4-15-99	17 51	31129	25 V	off	18 25	31143	Edgewood	off	Push Red Button
JML	4-15-99	18 10	31143	Edgewood	on	18:30	31159	25th V	OK	
JM2	4-16-99	7 36	31159	25 V	on	7.42	31161	Sierra	off	

Driver's OBDIII Vehicle Usage Log

Page: _____

Vehicle: Lumina

Driver's Initials	Date	Time of engine start	Odometer at engine start	Location at engine start	CEL at engine start	Time of engine stop	Odometer at engine stop	Location at engine stop	CEL at engine stop
FDG	4/15/99	17:36	27793	SIERRA	ON	17:59	27808	DAVIS	ON
FDG	4/16/99	7:35	27808	DAVIS	ON	7:58	27823	SIERRA	ON

Dan's mi: 530 753 7153

Driver's OBDIII Vehicle Usage Log — Page: ____

Vehicle: Breeze

Driver's Initials	Date	Time of engine start	Odometer at engine start	Location at engine start	CEL at engine start	Time of engine stop	Odometer at engine stop	Location at engine stop	CEL at engine stop
~~AE~~									
AE	4/12	4:39p	22987	Sierra	NO	507p	23003	Roseville	NO
~~AE~~	~~4/12~~	~~507~~	~~23003~~			—	—	—	—
AE	4/12	520p	23003	Roseville	NO	539 p	23013	Loomis	NO
AE	4/12	~~25~~1620	23013	Loomis	NO	638p	23022	Roseville	NO
AE	4/12	751p	23022	Roseville	NO	758p	23023	" "	NO
AE	4/12	912p	23023	" "	NO	918p	23024	"	NO
AE	4/13	811a	23024	"	NO	840a	23041	Sierra	NO
AE	4/13	540p	23041	Sierra	NO	552p	23045	Arden Mall	yes
AE	4/13	558p	23045	Arden Mall	yes	619p	23058	Roseville	yes
AE	4/14	813a	23058	Roseville	yes	845a	23075	Sierra	yes
AE	4/14	542p	23075	Sierra	yes	611p	23092	Citrus Hts	yes
AE	4/14	622p	23092	Citrus Hts	yes	630p	23095	Roseville	yes
AE	4/15	825a	23095	Roseville	yes	848a	23111	Sierra	yes
AE	4/15	558p	23111	Sierra	NO	622p	23128	Roseville	NO
AE	4/14	740a	23128	Roseville	NO	804a	23144		

Driver's OBDIII Vehicle Usage Log

Page: 1

Vehicle: Honda

Driver's Initials	Date	Time of engine start	Odometer at engine start	Location at engine start	CEL at engine start	Time of engine stop	Odometer at engine stop	Location at engine stop	CEL at engine stop
NK	4/12	4:48 pm	4729	ARB	No	5:00 pm	4734	Friend's	No
"	"	5:20 pm	4734	Friend's	No	5:34 pm	4737	CSUS	No
"	"	6:48 pm	4738	CSUS	No	6:56 pm	4741	Friend's	No
"	"	6:57 pm	4741	Friend's	No	7:19 pm	4749	Home	No
NK	4/13	6:03 am	4749	Home	No	6:23 am	4761	ARB	No
"	"	11:09 am	4761	ARB	No	11:19 am	4765	Post office	No
"	"	11:37 am	4765	Post office	No	11:43 am	4766	Store	No
"	"	11:59 am	4766	Store	No	12:16 pm	4771	ARB	No
HM	4/13	1:26 pm	4771	20th St	"	1:28 pm	4771	parking lot	No
T.A.	4/13	4:34 pm	4771	20th Street	NO	4:42 pm	4771	Sierra	NO
TA.	4/13	5:27 pm	4771	Sierra Plz	NO	5:28 pm	4772	20L	NO
T.A.	4/13	6:22 pm	4772	20th street	NO	6:53 pm	4795	Rocklin Home	NO
TA.	4/13	8:08 pm	4795	Rocklin home	yes	8:19 pm	4800	Rocklin Gym	yes
T.A	4/13	9:57 pm	4800	Rocklin Gym	yes	10:06 pm	4805	Rocklin store	yes
T.A.	4/13	10:16 pm	4805	Rocklin Store	yes	10:30 pm	4812	Rocklin Home	yes
T.A.	4/14	8:07 am	4812	Rocklin home	yes	8:12 am	4813	Rocklin School	yes
T.A.	4/14	8:20 am	4813	Rocklin school	yes	8:52 am	4835	20L	yes
TA.	4/14	11:29 am	4835	20L	NO	11:32 am	4835	Sierra	NO
TA.	4/14	12:21 pm	4835	Sierra	NO	12:26 pm	4835	20L	NO
HM	4/14	1:09 pm	4835	20L	NO	1:40 PM	4854	WORK	NO
			4854						
HM	4/14	3:36 pm	4854	Davis	NO	4:05 pm	4871	20L	NO
TA.	4/14	4:10 pm	4871	20L	NO	4:39 pm	4895	Rocklin home	NO
TA.	4/14	4:48 pm	4895	Rocklin home	NO	4:52 pm	4897	Rocklin park	NO
TA.	4/14	6:14 pm	4897	Rocklin park	NO	6:32 pm	4899	Rocklin home	NO
T.A.	4/15	8:02 Am	4899	Rocklin home	NO	8:07 Am	4899	Rocklin store	NO
TA	4/15	8:16 Am	4899	Rocklin store	NO	8:24 Am	4900	Rocklin school	NO
TA	4/15	8:27 Am	4900	Rocklin school	NO	8:57 Am	4922	20L	NO
TA	4/15	1:24 pm	4922	20L	NO	2:13 pm	4925	Sierra	yes
TA.	4/15	3:04 pm	4925	Sierra	yes	3:07 pm	4925	20L	yes
TA	4/15	6:00 pm	4925	20L	yes	6:05 pm	4926	19 & J	yes
TA.	4/15	6:13 pm	4926	19th & J	yes	6:40 pm	4949	Rocklin home	yes
TA	4/16	8:22 am	4949	Rocklin home	yes	9:19 am	4972	20L	yes
HM	4/16	11:17 am	4972	20L	yes	11:23 am	4972	20L	yes
HM	4/16	1:35	4972	20L	yes	1:50 pm	4972	Sierra	yes

Appendix D-4

Field Demonstration Summary

Summary of Results from Field Demonstration
Disablements - Onboard Detection - Remote Detection

System and Vehicle Date, Time, Disablements planted and removed by ARB	Detection of changes onboard by OEM's OBD system (CEL illumination)	Detection of change(s) onboard by OBDIII system	Logging of changes at Sierra via OBDIII
L1 Volvo			
4/14 1147 disable MAF	4/14 1745-1822	4/14 1745	4/14 1746 P0102 airflow sgnl vlts lo
4/15 1455 confirm P0102			
4/15 1456 clear code, reenable			
4/15 1459 disable TPS	4/15 1750-1815	4/15 1748	4/15 1748 P0123 TP circuit open
		4/15 1754	4/15 1755 P0120 TPS
L2 Sable			
4/13 1706 disable O2 sens.	4/13 1810-1824	4/13 1815	4/14 1111 P1151 undocumented code
		4/14 0753	4/14 1112 P0155 O2 htr bnk2,snsr1
4/14 1208 cnfrm P0155,P1151			
4/14 1212 clear code, reenable	4/14 1749-1800		
4/14 1215 disable MAF	4/14 1804-1821	4/14 1807	4/14 1807 P0102 airflow sgnl vlts lo
4/14 1442 confirm P0102			
4/15 1449 clear code, reenable	4/15 1734-1738	4/15 1739	4/15 1739 codes clear
4/15 1445 disable TPS	4/15 1751-1808	4/15 1810	4/15 1818 P0122 TP circuit short
L3 Lumina			
4/13 1658 disable TPS	4/13 1735-1745	4/13 1739	4/13 1740 P0122 TP circuit short
4/15 1451 confirm P0122			
4/15 1447 clear code, reenable			
4/15 1452 disable MAF	4/15 1736-1759	4/15 1740	4/16 1153 P0102 airflow sgnl vlts lo P0122 TPS ckt short

L4 Breeze			
4/13 1713 disable EGR vac.vlv.	4/13 1740-1752	4/13 1748	4/13 1750 P0403 EGR sol. ckt
4/14 1150 confirm P0403			
4/14 1153 clear code, reenable		4/14 1130	4/14 1205 codes clear
4/14 1202 disable chrgair/MAP		4/14 1203	4/14 1205 P0113 intake air temp hi
	4/14 1742-1811	4/14 1745	4/14 1747 P0108 MAP/baro ckt hi
4/15 1436 cnfrm P0108,P0013			
L5 Honda			
4/13 0807 disable TPS	4/13 0808-0819	4/13 1635	4/13 1636 no codes present
	4/14 0820-0852	4/14 0821	4/14 0822 P0122 TPS ckt short; P1790 undocumented code
4/14 0856 cnfrm P0122,P1790			
4/14 0857 clear code, reenable	4/14 1129-11:32	4/14 1130	4/14 1205 no codes present
4/14 1536 disable evap/EGR			
4/15 0827 disable evap/sol.	4/15 1324-1413	4/15 1409	4/15 1410 P0441 evap purge flow lo
4/15 1335 no codes			

APPENDIX E

Legal Analysis

sierra research

1801 J Street
Sacramento, CA 95814
(916) 444-6666
Fax: (916) 444-8373

April 27, 1999

Memo To: Tom Cackette, Chief Deputy Executive Officer
California Air Resources Board

From: Kingsley Macomber, General Counsel

Subject: Update on Legal and Public Acceptance Issues Associated with OBD III

This memo fulfills Sierra's commitment, under California Air Resources Board (CARB) Agreement No. 96-332, to provide an updated analysis of legal and public acceptance issues associated with the OBD III program.

"OBD III" refers to vehicle software and hardware that has the capability of transmitting emissions-related information in the vehicle's onboard diagnostics (OBD) system to the state via a wireless cellular communications link, as an alternative to on-site vehicle inspection under the current Inspection and Maintenance (I/M) program. In this memo, we briefly review Sierra's earlier legal analysis provided in 1993, based on a program using transponder technology. We provide a summary of the cellular area-wide communications technology that is being demonstrated under Agreement No. 96-332, and outline how the program would work. OBD III is then examined in detail in light of current federal and California constitutional law protections against unreasonable searches and seizures, and the right to privacy. We also discuss certain privacy principles and the California Information Practices Act of 1977, which could be important in determining public acceptance of OBD III.

It is Sierra's conclusion that a mandatory OBD III program, while potentially defensible against constitutional challenge, also presents substantial constitutional risks and, further, may not be publicly acceptable if it is mandated as a fully operational requirement for all vehicles. Accordingly, if OBD III capability is made a regulatory requirement, we recommend that vehicle owners or operators be given the option of activating or deactivating the system and complying with the regular I/M inspection requirements. There are also certain steps we recommend to address public acceptance concerns.

1993 Legal Analysis

Readers of this memo should refer to Sierra's previous draft memo analyzing OBD III legal issues. The memo, dated June 23, 1993 (Attachment A), was provided to CARB under an earlier contract between Sierra and CARB. The 1993 draft memo addressed, inter alia, the viability of an OBD III program using transponder technology in light of

two federal and state constitutional issues: the prohibition against unreasonable searches and seizures, and the right to privacy.* In general, the 1993 draft memo concluded that a transponder-based program should be constitutionally viable under the principles enunciated by the courts at the time, primarily because the program was not overly intrusive and any associated infringement on personal rights appeared to be justified by California's paramount and overriding interest in clean air. A key factor in that conclusion was the classification of automobiles by the courts as a highly regulated commodity for which there is a "diminished expectation of privacy." However, the memo further noted that the courts had never previously examined a program like OBD III involving large-scale, suspicionless electronic surveillance of private property, and that the previous legal precedents might be deemed inapplicable – thus creating an added element of risk in the event of legal challenge. The memo further suggested that public and legislative acceptance of the program was problematical.

The OBD III program reviewed in this memo is significantly different from the 1993 program, in that the communication technology chosen for the link between vehicles and government regulators for the current project uses cellular radio signals rather than short-range transponders. In addition, there have been a number of new court decisions in the search and seizure/privacy area that need to be reviewed.

1999 OBD III Technology

The OBD III system analyzed in the 1993 draft memo was based on short-range transponder technology. It was envisioned that a transponder would obtain a vehicle identification number (VIN) and OBD-related fault code information from vehicles using readers located (1) at I/M stations, where they would obtain data when a vehicle came in for a biennial or change-of-ownership inspection; or (2) alongside designated freeways and arterial roadways, where they would obtain information from vehicles as they drove by. The range of such a system would be no more than a few hundred yards, and OBD information would be obtained only from vehicles that passed within range.

In the updated system now under consideration, the vehicle computer will be programmed to constantly scan OBD data for a change in fault codes. The computer would also determine whether more than a specified time period (e.g., 90 days) has elapsed since the last data transmission. Whenever a change in codes is detected, or if the time period has been exceeded, the computer would attempt to transmit a radio signal over a wireless data network via a modem. The signal would consist of the fault code data, the VIN, and a date/time stamp. If the transmission is not successful, the computer would repeat its scan-and-transmit cycle. The result is that a transmission occurs only once every designated time period unless the fault code changes, in which event a transmission is immediately sent. A simplified schematic of the system is contained in Attachment B.

---

* The 1993 draft memo covered other issues such as FCC licensing, tort liability and questions regarding due process and equal protection, which will not be further addressed in this memo. The 1993 draft memo also concluded that the Board probably has sufficient aurhority under existing law to implement an OBDIII program.

There are numerous follow-up or enforcement mechanisms that could be implemented. If the state receives information that a vehicle has generated a fault code, it could immediately send the owner a notice by mail to have the vehicle repaired and require a certificate of compliance (C of C) to be submitted by a specified date or on the next annual re-registration. However, it is probably advisable to hold off sending any such notice until after a certain time has elapsed (e.g., 30-60 days) to allow the vehicle owner time to voluntarily to fix the problem without notice or involvement by the state. Under this latter approach, proper repair would be confirmed by a signal confirming that a previous fault code has been erased. If no such signal is received, then a repair notice can be sent to the owner.

The periodic signal, even if it contains no fault code(s), would serve as a safeguard against system failure and as a tampering deterrent; if it is not received in a timely manner, the state could notify the owner and either require a prompt I/M inspection or direct the Department of Motor Vehicles (DMV) to require a C of C on the next annual registration.

The wireless data network would be provided by an area-wide commercial cellular telephone or pager service provider under contract with the state. (Alternatively, the state could allow a vehicle manufacturer to assume the responsibility for data transmission using a private communications system built into the vehicles.) Using its network of radio towers, the cellular service provider (or the vehicle manufacturer) would receive the signal, analyze the data, and notify the state regarding vehicles with detected faults or the lack of a periodic signal. The system would obtain data from all OBD III-capable vehicles being driven in the service area of the cellular service provider, which currently would include all major urban areas in the state. By the time OBD III might become operational in several years, cellular service areas will probably be operating statewide. Thus the sweep of the program will be considerably wider, and involve many more vehicles, than would be possible under a transponder-based system.

During prototype field demonstrations, a separate dashboard-mounted driver interface will be built into the system that will use lights to indicate when a change in fault codes has been detected and when a communications link over the cellular provider's system is being activated. In production vehicles, the driver will be alerted that a fault code signal has been sent (or was attempted) by the illumination of the MIL; otherwise, operation of the system will not be apparent. The MIL would also alert drivers if the system has become non-operational or has been tampered, and is thus not capable of sending a periodic signal confirming its proper operation.

Under OBD III, vehicles with emissions-related problems would be repaired within a month or two of a fault or system deactivation being detected (or by the next re-registration deadline at the latest), instead of up to every two years under the current I/M program. Vehicles with OBD III capability would be exempted from the I/M inspection requirements. Eventually, after OBD III has been incorporated in most of the on-road vehicle fleet, elimination of the inspection portion of the I/M program may be possible.

The OBD III system could be designed as a two-way system capable of receiving and automatically responding to radio messages from the state (e.g., a query asking for any fault codes or a system status check), or from the vehicle manufacturer (e.g., software

modifications to improve or repair the vehicle computer voluntarily or under recall order from CARB). However, the capability of receiving incoming messages is not included in the system being demonstrated, and does not appear to be necessary. Similarly, the system would not be configured to retrieve and transmit other types of vehicle data (e.g., vehicle speed or location).*

Once implemented, and within budgetary and data processing limits, the OBD III system would allow CARB to receive real-time and periodic OBD information from millions of vehicles across the state, as often as necessary. The analysis of legal issues set forth below assumes that the OBD III program is mandated, i.e., that CARB adopts regulations requiring all vehicles, beginning with a specified model year, to have OBD III systems with capabilities similar to the system described above, and that enforcement mechanisms are implemented to require inspection and repair of vehicles found to have fault codes or de-activated systems, as described above. It should be mentioned, however, that most of the legal issues associated with a mandatory program can be avoided if OBD III is made voluntary. It is Sierra's understanding that allowing vehicle owners the option to participate in the OBD III program, as an alternative to biennial inspection, is one format for the program that is under serious consideration, at least for initial implementation. Further discussion of the more limited legal issues that could affect a voluntary program, and the types of optional programs that are available, is presented below under the section labeled Voluntary OBD III Program.

Constitutional Issues

Search and Seizure – Because the state would be mandating the retrieval and transmission of data from privately owned vehicles, the OBD III program immediately raises the question whether it violates the right against unreasonable search and seizure under the Fourth Amendment of the U.S. Constitution and the counterpart right in the California Constitution. Although they are not specifically mentioned, it is settled law that vehicles are covered by the federal and state constitutional protections against unreasonable searches and seizures. But there is a threshold issue whether OBD III is a "search." Generally speaking, in order for there to be a search under the Fourth Amendment, the U.S. Supreme Court requires that the person affected have a reasonable expectation of privacy relating to the information sought by the government. In cases involving motor vehicles, in recognition of their highly regulated nature and their mobility, the court has been willing to recognize only a limited expectation of privacy, and has allowed police to use electronic surveillance and other technology to locate and track vehicles on the road. In several cases, the court has characterized the use of electronic surveillance as no more

* Accessing such other types of vehicle information through the OBD III system would be technically possible, but is neither necessary to meet program objectives, nor desirable from a public policy standpoint. If such information is obtained, it would cause a quantum increase in both constitutional and public acceptability risks.

than an extension of surveillance by direct observation. In such cases, some courts have concluded that no Fourth Amendment "search" has even occurred.*

At first glance, OBD III would seem to fall within the scope of the cases described above allowing electronic surveillance of motor vehicles. However, OBD III goes beyond merely tracking vehicles: it requires information within the vehicle computer to be monitored and sent to the government. The information obtained through the OBD III program cannot be obtained simply by direct observation. While it could be contended that OBD III is no more than an extension of the biennial I/M inspection, such an argument would probably not be persuasive to a court. There definitely are other aspects of OBD III that require a more in-depth examination of its constitutionality. Due to its constant operation, its applicability to literally every vehicle on the road, and the fact that OBD III opens up access to the vehicle computer and sends data to the state automatically without any direct involvement by the vehicle owner or driver, we believe that a court would determine that the program is sufficiently different from I/M in how it works that it cannot be dismissed simply as another permissible form of I/M.

The breadth and automated operation of OBD III are perhaps its most constitutionally critical aspects. When the OBD III communications link is used to retrieve emissions data, the exercise falls into a category known as "suspicionless searches" under search and seizure law. Typically, these are cases where a search of a group or class of persons or their property is conducted even though no single person in the group or class is actually suspected to have participated in a prohibited or illegal activity. The OBD III program is a suspicionless search because CARB has no reason to suspect that a particular vehicle has a defective emissions control system or excessive emissions, but nevertheless requires the vehicle computer to monitor for and report information concerning compliance with CARB regulations. The program does not rely on externally sensed information, such as a smoking exhaust or carbon monoxide levels in the exhaust plume, to justify inspection. These kinds of cases are distinguished from cases where a search is based on "individualized suspicion" of wrongdoing, for example where an officer becomes suspicious when he or she sees a particular vehicle being driven erratically, and then acting on that suspicion stops the vehicle and conducts a search for alcohol or drugs.**

Federal Constitution -- The U.S. Supreme Court has made it clear in a series of decisions over the past decade that suspicionless searches, if certain constraints are met, are permissible in light of the prohibition in the Fourth Amendment to the US Constitution against "unreasonable searches and seizures."

As enunciated in a recent ruling of the court, Chandler v. Miller, 520 US 305 (1997), suspicionless searches are reasonable under the Fourth Amendment only where they are

---

* The cases and legal principles in this paragraph are discussed in more detail at pp. 13-14 of the 1993 draft memo.

** It could be contended that the program is in fact suspicion-based, because no reporting to CARB is undertaken unless the OBD system detects a fault. However, this view ignores the fact that the system will continuously monitor or "search" for faults or system deactivation even when there is no reason to believe that such a condition exists.

based on "special needs" beyond the normal need for law enforcement. In such cases, courts must undertake a "context-specific inquiry, examining closely the competing private and public interests advanced by the parties." In applying this special needs test, the court made it clear that suspicionless searches are warranted only under "limited circumstances" and that the category of permissible suspicionless searches is to be "closely guarded."

Under this litmus, the U.S. Supreme court has found comprehensive suspicionless drug testing to be permissible as applied to the following categories or persons: railroad employees (Skinner v. Railway Labor Executives Assn, 489 US 602, 1989); U.S. government customs employees (Treasury Employees v. Von Raab, 489 US 656, 1984); and college students who participate in interscholastic sports (Vernonia School Dist. 47J v. Acton, 515 US 646, 1995). In the Chandler case noted above, the court reversed the trend of the three previous cases and determined that mandatory drug testing by the State of Georgia of persons seeking to qualify for nomination or election to certain high level state offices was not permissible. In so ruling, the court found that drug testing was ineffective in deterring substance abuse in candidates and that public scrutiny of a candidate's behavior was a better alternative. In all four cases, the court closely examined the importance of the public interest asserted as the justification for drug testing, as well as the scope and method of testing and how directly it served the alleged public interest. Because of the subjective nature of the special needs test, and the requirement for the court to make such fact-intensive inquiries, the outcome of suspicionless search cases is unpredictable and fraught with court second-guessing of legislative and agency policy.

Another U.S. Supreme Court case, Michigan Dept. of State v. Sitz, 496 US 444 (1990), is perhaps the most relevant for assessing the constitutionality of the OBD II program, because it involved a motor-vehicle related activity: roadside sobriety tests. Such tests are another example of suspicionless searches, in that drivers are pulled over by police for testing, usually at a roadblock, in the absence of any suspicion of drug or alcohol use on the part of any individual driver. In Sitz, the court applied the same special needs test as it did in the above-cited drug testing cases, and determined that a properly designed roadside sobriety test was permissible under the Fourth Amendment because of the importance of preventing deaths and injury caused by drunk driving; however, it did so only after noting two important factors. First, the court observed that there was a "diminished expectation of privacy" in the case of operating motor vehicles on public roads, due to the highly regulated nature of vehicles as well as their highly mobile nature.* Second, the court relied on the absence of excessively intrusive procedures used by police in place for stopping vehicles and administering the sobriety tests. The court examined both the "objective intrusion" (i.e., how vehicles were selected, duration of the stop, nature or intensity of the sobriety test) as well as the "subjective intrusion" (i.e., the potential for causing "fear or surprise" or "concern" in motorists).

As noted above, there are a number of U.S. Supreme Court cases where electronic surveillance of vehicles has been permitted under the Fourth Amendment, but these cases

---

* See p. 13 of the 1993 draft memo for further discussion of how the court has recognized the diminished expectation of privacy in other automobile cases.

all dealt with suspicion-based surveillance of individuals, and not broad-based suspicionless testing programs.* These cases also involved enforcement against illicit drug activity, and could be distinguished from the OBD III program on that basis.

It is therefore our view that the OBD III program would present a novel set of facts were it to come before the U.S. Supreme Court for review. All of the suspicionless search cases decided to date have been drug- or alcohol-related cases; in this case, the public interest being protected is clean air, and the gravity or importance of the public interest in clean air has not been examined yet in the Fourth Amendment context. Likewise, the nature of the "offense" consists of a failed mechanical or software component that triggers an obligation to repair the offending vehicle (or at most, in the case of tampering, constitutes a minor infraction), as opposed to a serious criminal activity (drug purveying) or activity that can directly cause death or serious injury (drug use or drinking while driving). Electronic surveillance is involved, but in the context of a suspicionless search rather than a search based on individualized suspicion. And, perhaps most importantly, the class or group or persons subject to search is much broader, and the frequency and duration of the search is more extended, than in any case yet examined. OBD III will apply not just to a limited class of employees or students, or a few hundred drivers at a single roadblock on one night, but en masse to millions of vehicle owners, and will operate constantly on a day-after-day, year-after-year basis. The OBD III program has been reconfigured from short-range transponders in 1993 to now use cellular telephone/pager technology that presently can cover entire urban areas (and probably the entire state in the near future), and would enable nearly instantaneous reporting of fault codes and regular reporting of the system status. As such, OBD III constitutes a form of suspicionless mass electronic surveillance that has not yet been reviewed by the U.S. Supreme Court.

If the U.S. Supreme Court were to apply its special needs test to the OBD III program, there is a fair chance, but it is by no means certain, that the program could be found reasonable under the Fourth Amendment. Set forth below is a summary analysis of the issues that would likely be addressed in a Fourth Amendment examination of the OBD III program.

1. Importance of the State's Interest – The court will closely examine the objectives and purpose of the OBD III program, and independently determine whether they are important enough to justify the particular government intrusion. CARB should be able to demonstrate convincingly that clean air protects the public health and welfare, and that an important public interest is at stake. There are strong legislative statements proclaiming the importance of clean air in both the federal Clean Air Act and the California Health & Safety Code that the court should be willing to recognize.** It is possible the court would make some comparison to the importance of the public interest in

---

* See p. 14 of the 1993 draft memo.

** See, e.g., Health & Safety Code sec. 39000, where the Legislature states that the state has a "primary interest" in the quality of its physical environment; and Health & Safety Code sec. 43000, which states that the control and elimination of vehicular emissions is of "prime importance" for the protection of the public health and well being.

protecting sobriety in drug and alcohol cases; the outcome of such a comparison is hard to predict. It can be demonstrated that air pollution at the levels presently experienced in California, like drugs and alcohol, contribute to illness and even premature death; however, it is our sense that the adverse health effects of air pollution, even acknowledging their severity, could be characterized as less immediately debilitating to society. Another factor might be that air pollution in general, and OBD III specifically, is dealt with through non-criminal programs. If such a comparison were made, the court might be unwilling to tolerate as much intrusion as is allowed for searches to ferret out drug- or alcohol-related criminal activity.

2. Effectiveness and Necessity of OBD III for Clean Air – The court will examine closely whether and to what extent OBD III is necessary for achieving clean air objectives, and whether it truly serves those objectives. CARB will have to show why less intrusive alternatives, such as a program using shorter range transponders or roadside remote sensor devices, or a more effective version of the current I/M program that relies on periodic inspection at licensed garages or central stations, cannot adequately serve the same objectives. In this regard, actual quantification of the incremental benefits of OBD III compared to such alternatives will be important, and those benefits must be shown to be substantial.* Evidence in the record showing that the incremental benefits of the program are necessary for State Implementation Plan purposes would be highly useful.

3. Reduced Expectation of Privacy – While the court will likely acknowledge that the public has a reduced expectation of privacy with regard to motor vehicles, CARB will still have to demonstrate that OBD III falls within the scope of public expectations. To date, the Supreme Court has said that law enforcement officials can, in the absence of suspicion, stop vehicles for safety and sobriety inspections if adequate procedural safeguards are present. But OBD III may not be protected by those decisions because there is no actual stopping of the vehicle, i.e., the surveillance will be conducted without the knowledge of the vehicle owner or driver. Also, by accessing the vehicle computer itself, OBD III may be viewed as entering a more protected area.

   In defense of the program, CARB can assert that California is already implementing a vehicle I/M program that requires vehicles to be brought in for inspection biennially and on change of ownership. As noted, we do not think the OBD III program can be portrayed as merely an extension of the I/M program, but it could be contended nevertheless that it falls within individual expectations of how one's vehicle can be regulated. The safeguards discussed below under the topic of intrusiveness should also be helpful in showing that the public's privacy expectations have not been violated.

---

* It is Sierra's view that CARB can effectively demonstrate the comparative benefits of OBD III compared to the alternatives mentioned. Those benefits are further discussed in a separate report to CARB.

4. Intrusiveness -- In the Sitz case, supra, the U.S. Supreme Court focused in detail on the intrusiveness of the government search, both objective and subjective. It seems clear that the objective intrusion of OBD III is minimal, and certainly less than in the case of a sobriety roadblock. Drivers are not required to stop or otherwise alter their normal driving patterns, or have their persons observed or tested. However, there is a great potential for "subjective intrusion" – i.e., fear or concern that the government is constantly and secretly monitoring one's vehicle, or even that additional monitoring beyond emissions may be occurring secretly. In fact, the minimal physical intrusion of the program creates the potential for concern about subjective intrusion. CARB should not underestimate the potential strength of this concern, both in the mind of the public as well as the mind of a reviewing court.

   Fortunately, the subjective intrusiveness of the program can be reduced if certain public safeguard features are included, such as (1) written notice to vehicle owners, given at the time of vehicle purchase, that the vehicle has an OBD III system; (2) a clear description in the owner's manual of how the system works, as well as an explanation of what it does not do (e.g., that it cannot provide the location of a vehicle or allow control of the vehicle); (3) a form in the purchase documents, to be signed by purchaser, that the owner consents to the system by purchasing the vehicle;* (4) the presence of a MIL on the dashboard alerting the owner or driver that an OBD III fault code signal has been sent to the state; and (5) a form explaining the program that is provided with the annual DMV re-registration notice, plus regular media publicity. The first three recommendations were more fully discussed in the 1993 draft memo. The fourth and fifth recommendations are given due to the changeover to cell phone/pager cellular technology, which has the capability of operating even more broadly and secretively than a transponder-based system. Without this kind of public information, the OBD III program may not withstand the detailed scrutiny given by the Supreme Court to the intrusiveness of governmental searches.**

5. Electronic Surveillance -- As noted above, the U.S. Supreme Court has accepted the use of modern electronics in cases involving vehicles driven by individuals suspected of illegal activity. These cases involved beepers, aerial surveillance, and other devices that were accepted by the court because they merely enhanced or automated the ability of the police to monitor vehicular activity directly (e.g., by following or watching the individual in question). However, there is clearly a line beyond which the court will not tolerate electronic surveillance. In U.S. v. Karo, 468 US 705 (1984), the court said it

---

* The owner's consent could constitute a complete defense to a Fourth Amendment challenge, but only if it is accepted as valid by the court. Based on the decisions to date, the court does not seem willing to focus on the consent issue; accordingly, obtaining vehicle owner's consent may be more useful in addressing the expectation of privacy issue.

** In People Banks, 6 Cal. 4th 926 (Dec., 1993) the California Supreme Court ruled that the Sitz decision does not require advance publicity of a sobriety roadblock. However, failing to give the public adequate advance information about the OBD III program would clearly create unnecessary risks, given the unique and extremely broad scope of the program.

was permissible for police to use a beeper placed in a drug container to follow a drug suspect to his house, but not to determine whether contraband was actually in the house. That case may be distinguishable as involving a person's home (considered a special sanctuary under the Fourth Amendment), as opposed to a motor vehicle that moves about in open view and is the constant subject of observation and regulation. But Karo, and the fact that OBD III takes electronic surveillance into the uncharted waters of suspicionless mass surveillance, may tempt the court to find that the line of impermissibility has been crossed.

6. Confidential Use of Data – Proper use of information obtained in a suspicionless search is another factor that appears to be required for the search to be deemed reasonable under the Fourth Amendment. For example, in the employee and student drug testing cases mentioned above, the U.S. Supreme court noted approvingly that test results, as well as any disciplinary proceedings that might occur as a result of testing, were kept confidential. There is a similar concern that could arise in the OBD III program. Individuals who receive a notice requiring them to repair their vehicles could be upset or concerned if third parties can learn about their receipt of the notice. Other agencies such as the Bureau of Automotive Repair (BAR), the California Highway Patrol (CHP), CalTrans, or local, state or federal criminal investigators, may want access to use data generated by the program, or to use the communications link for their own data-gathering purposes. If these issues are not addressed, they could raise collateral Fourth Amendment risks. Accordingly, the CARB regulations establishing the program should contain specific confidentiality safeguards for data and compliance actions, and CARB should maintain independence from any other agencies' efforts to piggyback onto OBD III.*

One final caveat: because the OBD III program is so unique from the perspective of constitutional law, it is possible that the Supreme Court will develop a different and perhaps more stringent constitutional test. For example, it could state that the search must be justified by a compelling state interest and that there must be no alternative for achieving that purpose; or perhaps the court would require express findings of necessity by the state Legislature and not by a regulatory agency. If this approach is taken by the court, even the most careful consideration of the factors discussed above may not be sufficient.

California Constitution – Like the Fourth Amendment to the U.S. Constitution, the California Constitution, in Article I, Section 19, also prohibits "unreasonable searches and seizures." The California Supreme Court is the final arbiter of the meaning of this provision, and can interpret it differently than the U.S. Supreme Court interprets the same wording in the Fourth Amendment. In its decision in Loder v. City of Glendale, 14 Cal. 4th 846 (1997), a case involving mandatory drug testing by the City of Glendale of job

* Compliance with the California Information Practices Act of 1977, discussed infra, should help to effectively address the confidentiality issue.

applicants as well as existing employees who are seeking promotion, the California Supreme Court issued its most recent guidance on suspicionless searches under Article I, Section 19. In Loder, the California Supreme Court adopted the same "special needs" balancing test used by the U.S. Supreme Court under the Fourth Amendment, citing the Skinner, Van Raab and Vernonia decisions of that court previously discussed. The court's special needs analysis resulted in a finding that the City of Glendale could require drug testing of job applicants, but that the city's justification for across-the-board testing of all categories of current employees was not important or convincing enough to justify the intrusion. In reaching this conclusion, it was noted that comprehensive testing of job applicants was reasonable because the City had no other reliable source of information about their behavior; whereas for current employees, the court was persuaded that the City would be able to evaluate their behavior based on their previous performance on the job.

The principal message of the Loder decision, aside from confirming that the same legal test applies for a search and seizure case under the California Constitution as under the U.S. Constitution, is that any evaluation of the OBD III program will be fact-intensive. The court will examine the importance of the interest that is being advanced by the state to justify the suspicionless search, whether and how much the search advances that interest, the scope and intrusiveness of the search, how the information is used, and whether there are alternative, less intrusive means for obtaining the same information. This means that any decision by the state Supreme Court on OBD III cannot be predicted in advance. But it also suggests that all aspects of the program should be designed carefully to withstand close personal scrutiny by all the justices. How this might be done is addressed above, under the issue analysis for meeting the U.S. Supreme Court's requirements.

The California Supreme Court has also recently changed its approach to search and seizure cases involving motorist sobriety checkpoints in a manner that could be relevant to the OBD III context. Over ten years ago, in Ingersoll v. Palmer, 43 Cal. 3d 1321 (1987), the court upheld the constitutionality of a roadside sobriety checkpoint operated by the City of Burlingame Police Department because the procedure complied with eight specific factors or safeguards imposed by the court to assure minimum intrusiveness on individual liberties.* Subsequently, in People v. Banks, 6 Cal. 4th 926 (1993), the California Supreme Court reviewed a sobriety roadblock operated by several police departments in the Seal Beach area. In upholding the roadblock, the court applied the same balancing test used by the U.S. Supreme Court in the Sitz case (supra), and determined that the roadblock was permissible despite the absence of advance publicity, which was one of the eight elements listed in its previous decision in Ingersoll. The court noted that advance publicity was not constitutionally required because the U.S. Supreme Court in Sitz focused on the duration of the stop, the intensity of the investigation, and other features such as "officialness" and the regular detainment of other motorists. The upshot of the Banks case is that the California Supreme Court abandoned the formulaic approach of Ingersoll for the more fact-based ad hoc approach taken in the Sitz case.

---

* The eight factors were as follows: operation in accordance with overall plan established by supervisory personnel, neutral formula for selection of vehicles, adequacy of safety procedures, reasonable site selection by supervisory personnel, reasonable time and duration, "officialness" of the checkpoint, minimal detention of motorists, and advance publicity.

This would seem to emphasize or increase the risk or unpredictability of a search and seizure decision under the California Constitution, and to buttress our suggestion that the OBD III program be carefully designed to eliminate all possible elements that could become an underpinning for constitutional rejection. The same design considerations discussed above under the Fourth Amendment would therefore apply to OBD III under Article I, Section 19.

Right to Privacy – As explained in the 1993 draft memo,* there is no explicit right to privacy under the U.S. Constitution. Nevertheless, the U.S. Supreme Court has inferred a right of privacy under highly limited circumstances, in cases involving "fundamental rights" or highly personal areas such as lifestyle, sexual activity, and pregnancy. Absent the creation of a new implied right to privacy in mass surveillance cases, a person's vehicle would therefore not fall under the protection of a federal right of privacy, as the right is presently construed by the U.S. Supreme Court.

However, the California Constitution does contain an independent right to privacy:

> All people are by nature free and independent, and have certain inalienable rights, among which are those of ... pursuing an obtaining safety, happiness and privacy. (Article I, Section 1. Emphasis added; emphasized words added by Initiative in 1972.)

At the time of the 1993 draft memo, the California Supreme Court had provided little guidance on the scope of protection provided under Article I, Section 1. Subsequently, in the 1994 decision of Hill v. National Collegiate Athletic Assn, 7 Cal 4th 1, the court instructed that one must initially consider the "kind of privacy interest" at stake. If the privacy interest is deemed "fundamental to personal autonomy," then the state must show a "compelling justification." If the privacy right is less central or disputed, then a "general balancing test" is to be employed. The court also noted that the right to privacy included "informational privacy," i.e., the right not to provide certain information to the government. The court then went on to explain the analytical process for examining whether the particular state activity is in violation of the right to privacy. First, the plaintiff must establish that a legally protected privacy interest is at stake, that he or she had a reasonable expectation of privacy, and that a serious invasion of privacy has occurred. The state must then prove that its invasion of that privacy is justified under either the compelling interest or balancing test, as appropriate, and that there are no feasible or effective alternatives involving a lesser intrusion on privacy.

The Hill case involved the question of whether the NCAA could mandate urinalysis drug tests as a condition of participation in college sports. Under the above approach, the court found that while the right of college athletes to participate in sports programs was not a fundamental right, such participation did qualify as both personal autonomy and informational privacy interests. But the court then ruled that drug testing through urinalysis was a legitimate and important interest, underlying the health and safety of student athletes as well as the integrity of intercollegiate sports, and that college athletes

---

* See 1993 draft memo at pp. 18-19.

have a diminished expectation of privacy with respect to drug testing. The court therefore upheld the NCAA urinalysis drug testing program.

Later, in the 1997 Loder decision, supra, a plurality of the California Supreme Court applied the balancing test in ruling that requiring a job applicant (as distinguished from existing employees) to take a drug test before being hired was not an unreasonable privacy intrusion. Also, in 1997, the court ruled in American Academy of Pediatrics v. Lundgren, 16 Cal 4th 307, that legislation requiring parental consent for a minor to have an abortion violated the minor's right of privacy under Article I, Section 19. In so ruling, the court noted, at least in the highly personal context of a procreative choice case, that the California Constitution confers significantly broader rights than the comparable right under federal law, and reinforced the view, even where the individual right of privacy at issue is a compelling one, that the court must still weigh and balance the justification for the state's intrusion against the individual's right to privacy.

These recent right-to-privacy cases involved split decisions of the court as well as differing views of the meaning of the seminal Hill case. It is difficult to reconcile all the decisions and views, but the best distillation is probably that the court will apply a fact-specific balancing test under which the importance of the particular right to privacy being asserted is weighed against the state's interest in obtaining the information sought to be kept private. In conducting the balancing test, the court will evaluate how important the right to privacy is, and require a stronger interest on the state's part if the individual right to privacy is personal and/or compelling. Given the inherent subjectiveness of the balancing test, the best approach for considering how OBD III would fare under the state's right to privacy is probably to state the issue as one of strengths and weaknesses. In favor of OBD III are the strong interest of the state in improving and protecting air quality, and the established principle that vehicles are associated with a reduced expectation of privacy. There is probably a potential for healthy air to be categorized as a "compelling" state interest, although that is by no means certain. Against OBD III are the fact that it involves a broad-based suspicionless search, and that alternative measures may exist that are nearly as effective but less intrusive.

Public Acceptance

In designing and implementing the OBD III program, CARB should take into account the likelihood of a strong, adverse public reaction. Because it potentially involves continuing governmental electronic surveillance on an unprecedented scale – involving millions of vehicles on an annual basis – the program is certain to be controversial and could become a lightning rod for criticism. In most any form, it will be given close scrutiny by many citizens and organizations, industry, the press, and the Legislature. The fact that it may be able to pass constitutional muster before the courts under the search and seizure and privacy principles discussed above does not assure public acceptance.

This portion of the memo therefore addresses a number of program policy considerations and options that could beneficially affect public acceptance of OBD III.

Cooperation With Privacy Watchdog Organizations - There is a well-organized network of private organizations in California and the U.S., and internationally, that are dedicated to protecting individual rights to privacy, and that actively monitor for government activities that may encroach unduly on those rights. These organizations typically focus on such areas as computer and internet use, consumer credit, telephone and wireless communications, and electronic surveillance. Where appropriate, they will become involved in state and national legislative processes, and will on occasion instigate litigation. One or more of these organizations could bring or become involved in a test case challenging the constitutionality of the OBD III program. Organizations in this category include the following:

- The Electronic Privacy Information Center (EPIC), in Washington, D.C.;
- The American Civil Liberties Union (ACLU), in New York City;
- Computer Professionals for Social Responsibility, in Palo Alto;
- Electronic Frontier Foundation, in San Francisco;
- Privacy Rights Clearinghouse, in San Diego;
- US Privacy Council, in Washington, D.C.;
- US Public Interest Group (PIRG), based in various states, including California (CalPIRG); and
- Intelligent Transportation Systems America (ITSA), in Washington, D.C.

There are also a number of academics and other thought-leaders who regularly publish on the topic of privacy rights and policy in papers, professional journals, and law journals.

While these sources are potential adversaries of OBD III, there may be an opportunity for CARB to establish a dialogue with one or more of these groups or individuals, prior to final program design and implementation, so that their suggestions can be taken into account. PIRG, for example, focuses on environmental as well as privacy issues, and may be a potential supporter for a program that can achieve privacy as well as environmental objectives. The organizations based in California may also be more amenable to accepting OBD III as a program that achieves needed environmental goals. It may be feasible to head off opposition by these sources through early communications and cooperation; however, even if that is not possible, a stronger program – one that is more capable of withstanding legal or legislative overview – may result.

Consideration of Privacy Principles – In designing the final version of the OBD III program, it would be advisable for CARB to give consideration to basic privacy principles that have been developed by privacy advocates. These principles have been used or adopted by entities such as the European Union, various federal agencies, and the City of San Diego in establishing policies for other issues involving privacy concerns, such as consumer credit, telecommunications, and the like. Last year, the Privacy Rights

Clearinghouse presented a list of nine comprehensive principles to the California Joint Legislative Task Force on Personal Information and Privacy* that could be addressed in the context of OBD III:

- Proactivity – Consideration of privacy issues prior to program adoption, i.e., conducting a "privacy impact assessment" as part of the program adoption process.
- Secondary Use – Prohibiting or limiting use of information for other than the purpose for which it was collected, except where affirmative consent is obtained.
- Access – Providing information about the policies and practices that govern how the agency manages information, and allowing the affected persons to review and correct information about them.
- Affirmative Consent – Collecting, using, and releasing information only with the knowledge and consent of the affected person.
- Relevance – Limiting information collected to that which is necessary to achieve the purpose of the agency, and retaining information only as long as necessary.
- Accuracy – Assuring that information is sufficiently accurate, complete, and up-to-date as necessary to achieve the purpose of the agency.
- Security – Safeguards against unauthorized access to, use, collection, disclosure, or disposal of information.
- Accountability – Designation of a person, and an enforcement mechanism, to assure proper management of information, and to serve as a contact with the affected public.
- Progress – Regular review of and changes in how information is managed in light of technology advances and program experience.

A similar list of eight principles has been published by ITSA (Attachment D).

Some of these principles would appear to be more important to the OBD program than others, but all of them should be considered. In particular, the issues of secondary use and relevance should be given close attention in light of concerns that have been expressed about use of the OBD III connection to the vehicle computer and its external communications link by other agencies (e.g., traffic enforcement agencies or criminal investigators) for non-emissions purposes such as controlling driving behavior or

* A more detailed explanation of these principles, taken from the Privacy Rights Clearinghouse website at www.privacyrights.org., is included as Attachment C.

monitoring the whereabouts of citizens. Likewise, establishing an accountable public contact point could be quite helpful in providing accurate information about how the program works, how abuses are being prevented, and preventing misunderstandings about the program.

Compliance With California Information Practices Act of 1977 – Like other state agencies, CARB is subject to the California Information Practices Act of 1977 (Civil Code secs. 1798-1798.78). This act, patterned after the federal Privacy Act of 1974 (5 USC 552a), contains basic strictures on how agencies are to handle "personal information." The act addresses many of the privacy principles described above. For example, agencies may keep only that personal information "relevant and necessary to accomplish a purpose of the agency," and must strive to obtain information "directly" from the affected individual (secs. 1798.14, 1798.15). Agencies must maintain the source of their information (sec. 1798.16) and maintain the "accuracy, relevance, timeliness and completeness" of their records (sec. 1798.18). Individuals from whom information is sought must be given a notice explaining certain specifics about why, by whom, and for what purpose information is being sought, as well as how the information will be disclosed and what rights of access exist for the individual (sec. 1798.17). There must be rules of conduct for agency employees who handle personal information, security and confidentiality safeguards, and a designated responsible employee (secs. 1798.20, 1798.21 and 1798.22).

The act goes on to set up detailed requirements for how agencies may and may not disclose personal information (secs. 1798.24-1798.24b), account for disclosures (secs. 1798.25-1798.28), and allow for individuals to access, review, and correct information (secs. 1798.30-1798.44). If an agency violates the act, the affected individual may bring a civil action seeking injunction and damages (including attorneys' fees and costs), and persons other than agency employees who wrongfully disclose personal information are also subject to a civil action for damages, including exemplary damages. Agency employees can be disciplined for a violation of the act, and it is a misdemeanor for any person to obtain personal information from an agency under false pretenses.

It is not clear that information obtained by CARB through the OBD III program would be subject to the act. As noted, the act applies to "personal information," which is defined as "information that is maintained by an agency that identifies or describes an individual," including such information as name, home address or phone number (sec. 1798.3(a)). Under OBD III, CARB will be obtaining only the vehicle identification number (VIN), a time and date stamp, and any emission control system fault codes stored by the OBD II system. Strictly speaking, this is information about the vehicle and not information about the owner or operator; however, the VIN will allow CARB to directly obtain personal information, i.e., the name and address of the registered owner of the vehicle. In the case of a vehicle with a fault code or status problem, CARB's files will contain further personal information about actions taken (or not taken) to have the vehicle repaired and certified through the issuance of a C of C. Given that information about the registered owners of vehicles and their driving records are expressly treated as "personal information" under the act (see sec. 1798.24(m)) and are subject to explicit statutory requirements concerning how it may be handled by DMV (see Vehicle Code secs.1800-1821), there is a fair chance a court would determine that information obtained through

OBD III is personal enough in nature, or would lead to CARB obtaining such information in a direct enough manner, that it is in fact "personal information" subject to the act.

In light of the potential for application of the Information Practices Act to OBD III, as well as for public and legislative acceptance reasons, it would seem advisable for CARB to design the program so that it complies with the act to the maximum extent possible.

Coordination with the Legislature – As noted above, the Legislature has appointed a Joint Legislative Task Force on Personal Information and Privacy. The task force is currently chaired by Senator Debra Bowen. Earlier this year, Senator Peace (the task force chair in 1998) introduced SB 129, to enact the "Information Practices Act of 1999." The bill is still in the process of being amended, but in its original form introduced further restrictions on the collection and use of personal information by state agencies, including the requirement that personal information may be collected only with the informed consent of the individual. If this requirement is enacted and the 1999 act is deemed applicable to OBD III information, it could have the effect of prohibiting a mandatory program. Other concepts addressed in the bill include the right for individuals to choose whether and how information about them is to be provided to third parties; additional measures to be taken to assure reliability of information and to prevent its misuse; improved access to information by affected persons; and the establishment of a statewide privacy ombudsman in the Department of Consumer Affairs.

In Sierra's view, there is no question that the Legislature will examine the OBD III program at some time prior to its implementation. It may be in CARB's interest to establish an early working relationship with key legislators, and in particular the chair and other members of the task force, in order to determine the extent to which and for what form of the program legislative support exists.

Coordination with Automotive Industry – If CARB decides to allow manufacturers to use their commercially developed proprietary communications systems in place of a state contractor, then clearly there must be full coordination with industry. But even if that option is not pursued, an OBD III program that has some support (or at least no opposition) from the auto industry would be easier to implement than one that is opposed by the industry. Vehicle manufacturers are now offering communications systems, e.g., GM's Onstar, that can send personal or vehicle information to external recipients via a wireless link, and the capabilities and use of such systems are expected to expand rapidly in the near future. Recently, several major manufacturers agreed to common software and hardware protocols for equipping their vehicles with "multimedia" capabilities,* including external communications. If OBD III is mandated (or if giving vehicle owners the option of using OBD III is mandated), the system will be integrated with the vehicle computer and communications systems. Coordination of CARB's objectives for OBD III and the manufacturers' objectives for a versatile, user-friendly communications package will be necessary for technical reasons alone. At the same time, manufacturers' views on how OBD III can be implemented in the least threatening manner for owners should be sought.

---

* GM, Toyota, Ford and DaimlerChrysler announced the agreement on April 26, 1999. Other manufacturers, including Ford and Volkswagen, are expected to become participants in the near future.

One segment of the industry, the aftermarket manufacturers, already appears to be highly critical of the OBD III concept. SEMA, the Specialty Equipment Manufacturers' Association, views OBD III as an expansion of an OBD II program that is already incompatible with the installation of many aftermarket products, and has published warnings on its website that OBD III could violate constitutional rights. There are (inaccurate) descriptions from industry members of how police would use the OBD III system to locate and arrest suspects, and to immobilize vehicles. The independent service industry is another likely opponent, given the potential for OBD III causing a dramatic reduction in the number of vehicle "smog"inspections. While it may not be possible to eliminate opposition from all industry segments, CARB should consider opening lines of communication to all industry groups prior to commencement of the regulatory process, including those that are against OBD III, in order to better understand how the program will affect the nature of industry and, to the extent possible, accommodate their concerns.

Voluntary OBD III Program

Implementation of OBD III on a voluntary basis should eliminate most, if not all, constitutional issues. It is highly doubtful that a valid search and seizure or privacy claim could be asserted where the system can be deactivated (or activated) at the option of the vehicle owner or operator. Public acceptance would also be improved if OBD III were instituted on a voluntary basis, although some resistance should be expected on the theory that voluntary implementation is but the first step toward a mandatory program.

There are a number of different ways in which OBD III could be made voluntary:

- Manufacturer Decides - Vehicle manufacturers could be allowed to decide whether to offer OBD III as a mandatory or optional system on their vehicles, subject to the requirement that it must meet specifications set by CARB if it is installed. Manufacturers' efforts to market the system could provide some credibility and help improve public acceptance. A drawback to this approach is that if OBD III is not OEM-installed, the vehicle owner, or a subsequent owner, would be prevented from later deciding to participate in the program (or have to make a substantial expenditure for retrofit).

- Vehicle Owner Decides - OBD III systems could be mandated for all vehicles of a certain model year and later, with the decision to deactivate or activate the system left up to the original purchaser (or a subsequent purchaser) at the time of purchase or later. This approach would appear to offer the maximum flexibility to the consumer, and therefore the least public resistance.

- Vehicle Driver Decides - OBD III systems could be mandated for all vehicles of a certain model year of later, with the decision to deactivate or activate the system left up the operator on an individual drive basis (subject to a minimum activation or automatic reporting requirement of, say, once per quarter).

The primary incentive to be offered for participation in a voluntary OBD III program would be exclusion from the I/M biennial inspection requirement, perhaps along with elimination of the new-vehicle exemption currently in effect for I/M. Exemption from the change-of-ownership inspection requirement could be another incentive. Other incentives, such as reduced inspection and certificate fees and/or repair cost subsidies, might also be considered. A final incentive would be to require the manufacturer to offer consumers without charge the option of having the system, if activated, provide vehicle location in the event of theft and/or air bag activation.

Moreover, even in a voluntary program, CARB should consider implementing the privacy safeguards that would be included in a mandatory program. This would mean incorporating features that address the privacy principles described above as well as the basic elements of the Information Practices Act of 1977. (If the act applies to OBD III information, it would apply regardless of whether the information is received voluntarily or through a mandated program.)

Conclusions and Recommendations

We believe that a mandatory OBD III program is likely to be challenged as unconstitutional. It is difficult to predict how the program would fare in such a case under the balancing test applied by the U.S. and California Supreme Courts, where the air quality benefits of the program would be weighed against the impingement on personal rights. As a potentially very effective emissions reductions measure, OBD III could be defended as a strong if not compelling interest of the state; however, at the same time, it is so broad that the threat to personal rights posed by the program could be viewed as intolerable. It is questionable whether a program so at risk to constitutional challenge should be adopted.

An even greater risk probably exists in terms of public acceptance. Despite the emissions benefits of the program, we doubt that the general public, privacy advocates, affected industry, or the Legislature will support mandatory OBD III, and many of these groups will oppose it. Primarily, the opposition would come from fears, perhaps more subjective than objective, about excessive government intrusion or merely the potential for such intrusion.

The solution to these risks would appear to be a voluntary program, coupled with an exemption from biennial and/or change of ownership I/M inspections as the primary incentive for participation. The schematic in Attachment B illustrates how system deactivation by the owner or driver can be included. As long as consumers are properly and fully informed about how the system works and how it affects them personally, a voluntary program should effectively eliminate the risk of constitutional challenge. A voluntary program would not eliminate all public opposition, but could be sufficient to prevent legislative intervention; however, if a voluntary program is implemented, it should still incorporate safeguards reflecting the privacy principles noted above and the basic elements of the Information Practices Act of 1977, in order to assure that data obtained under the program are properly managed and protected. Even in a voluntary format, two key protections should be provided: first, CARB must provide adequate

assurances (preferably through technical limits imposed on the program) that the capability for determining vehicle location is not used by the government;* and second, CARB must address the "relevance" principle and assure that the system is used only by CARB to obtain emissions-related data, and not by other agencies for other purposes. In particular, it needs to be demonstrable that OBD III cannot be used for criminal or investigatory purposes or to control vehicle operation.

Sierra's general recommendation for the preferred type of voluntary program is that all vehicles should be mandated to have OBD III capability, with the decision to deactivate that capability left to the vehicle owner or driver. We will address this recommendation in further detail in our separate technical report following completion of the field demonstration.

* It should be recognized that determining vehicle location is an inherent capability of any cell-phone or pager-based system. CARB will therefore have to consider taking affirmative steps to prevent vehicle location information from being generated or forwarded to it through the OBD III system, even though it cannot prevent the wireless service provider from having the capability for generating such information.

Attachment A

June 23, 1993

sierra research

1521 I Street
Sacramento, CA 95814
(916) 444-6666
Fax: (916) 444-8373

Memo To: Mark Carlock, ARB Mobile Source Division

From: Kingsley Macomber

Subject: Draft Legal Analysis of Transponder Program

Under the 1992-93 Task Order contract, Sierra committed to provide a legal analysis of the transponder program presently being developed by GM Hughes for the ARB. Enclosed you will find a draft analysis for your review and comment. This analysis will ultimately be incorporated in our full report to ARB on the transponder program later this year.

Please call if there are any questions.

encl.

DRAFT

Legal Aspects of Transponder Technology[1]

Introduction

Task 2 of Sierra Research's 1992-1993 Task Order contract with the California Air Resources Board (ARB) requires Sierra to undertake Feasibility Assessment, Fabrication and Demonstration of Radio Transponders for Inspection and Maintenance. In the Task Order approved by the ARB, Sierra committed to provide a legal analysis of transponder technology covering licensing, liability, constitutional and other issues. This report is provided in fulfillment of that commitment.

Licensing

Equipment - The prototype transponder equipment under evaluation consists of two separate two-way units designed by GM Hughes: a roadside reader and a small transponder for placement onboard a vehicle. The system uses a digital time division multiplexing/"slotted aloha" protocol to provide high-speed, accurate transmissions, and is capable of retrieving information from 12 lanes of bumper-to-bumper traffic travelling over 100 miles per hour. The reader will transmit at a maximum of 100 milliwatts, and the transponder at a maximum of 10 milliwatts. These are very low power signals, with a maximum range for the reader of about 150 feet.

Both units will be "spread spectrum" devices configured to broadcast in a frequency band of 915±13 MHz. This band was selected for its superior propagation characteristics. Spread spectrum devices have the capability of operating on different frequencies within a relatively wide band of available frequencies. The frequency used may vary from one transmission to the next. Different codes are also available to send messages on any given frequency, and the system includes a cyclic redundancy check (CRC) function to check for proper transmission of messages and repetition of messages not properly transmitted. In combination, these features allow the system to resist interference from other, higher-power signals using the same frequencies. Frequency assignment can be by random frequency hopping, by direct sequencing, or

---

[1] This report has been principally prepared by Sierra's in-house legal counsel. It is not written as a formal, definitive legal opinion, but is intended to establish legal parameters and identify issues in a fashion that will guide the ARB in deciding whether and what kind of transponder program it should adopt.

a combination (hybrid) approach. The prototype will principally use direct sequencing, but also has the capability of random switching between three separate frequencies. Spread spectrum technology is well suited to roadside monitoring because it allows the use of low-cost systems capable of reliably sending and receiving signals within a limited area, such as across several lanes of traffic.

The signal would transmit information stored in vehicle on-board diagnostic (OBD) systems. The information could simply be an indication of whether a fault code has been recorded, or could include actual fault code data.

For use in production units, Hughes is planning to upgrade the reader unit to 4 watts, and the transponder to about 100 milliwatts. The signal would be converted from spread spectrum to a coherent signal at 915±6 MHz. This approach is expected to extend the range of the system to cover all road configurations that might be encountered in actual use.

Spread Spectrum Requirements - Under the spread spectrum rule as revised in 1990 by the Federal Communications Commission (FCC; 47 CFR 15.247), spread spectrum transmitters that operate within three specific bandwidths (902-928 MHz, 2400-2483.5 MHz and 5725-5850 MHz) with no more than 1 watt peak power output fall within the "public range" and are exempt from user licensing. The spread spectrum rule was revised in 1990 to increase the maximum power limit to 1 watt in a specific attempt to encourage commercial development of low-power, short-range spread spectrum communications, but in doing so, the FCC also imposed new requirements relating to power density, processing gain, and minimum bandwidth separation, in order to prevent interference with licensed signals. The intent of the FCC spread spectrum regulation is to encourage innovative uses. Other examples of spread spectrum technology include cordless telephones, wireless inventory systems in warehouses, automated pricing systems in grocery stores, electronic clipboards in hospitals, fire and burglar alarms, and cableless office PC networks. New products are emerging on a regular basis.

According to the FCC, unlicensed spread spectrum broadcasts operate on a "noninterference" or permissive basis, meaning they have no rights if they cause interference with any kind of licensed signal. If an actual conflict develops, the spread spectrum user is responsible for eliminating the interference.

The prototype equipment has been designed to meet all FCC spread spectrum specifications. Thus, the prototype system will not require licensing of either the reader or transponder unit. If this equipment is retained in production units, the ARB as well as vehicle manufacturers and owners will not be required to license any equipment. However, the manufacturer of any spread spectrum equipment used in an ARB transponder program must obtain a Grant of Equipment Authorization from the FCC before sale or use of spread spectrum equipment (see Subpart J of Part 2 of 47 CFR). The grant requires a formal application, with test data showing compliance with FCC spread spectrum specifications.

Interference Issue - Spread spectrum technology shares its 902-928 MHz band where the ARB transponder system would operate with many other forms of radio transmission, including government agency signals, industrial/scientific/medical (ISM) users, and radiolocation devices, thus raising the question of interference. In a note to its spread spectrum rule, the FCC states:

> NOTE: Spread spectrum systems are sharing these bands on a noninterference basis with systems supporting critical Government requirements that have been allocated the usage of these bands, secondary only to ISM equipment operated under the provisions of part 18 of this chapter. Many of these Government systems are airborne radiolocation systems that emit a high EIRP which can cause interference to other users. Also, investigations of the effect of spread spectrum interference to U.S. Government operations in the 902-928 MHz band may require a future decrease in the power limits allowed for spread spectrum operation.[2]

Because this note has implications not only with respect to the feasibility of a vehicle emissions transponder program, but with respect to the liability question discussed below, Sierra contacted the FCC[3] to ascertain whether interference is, in fact, a significant problem. Theoretically, a spread spectrum transmission could interfere with any licensed broadcast on the same frequency, such as a commercial broadcast signal, government agency signal, police transmission, or even a traffic light control signal. However, the FCC presently has no proposals to constrict spread spectrum use, whether in the form of reduced maximum power requirements or otherwise. Its current position is that meaningful interference with licensed signals is "extremely unlikely", for several reasons. First, interference with other signals will be minimized by low power requirements. The prototype system being tested by the ARB vendor, GM Hughes, will be operating at no more than one-tenth the allowable maximum power. Second, the interference caused by a low-power spread spectrum system mainly appears as "noise" to more powerful external systems operating on the same frequency — i.e., the range of the external system may be somewhat affected, but direct interference ("butting-in") will not occur. Thus, interference caused by an ARB transponder system would become an issue only if the reader were located very close to a licensed receiver that is in a fringe reception area, and then only if both systems use identical or nearly identical frequencies at the same time. The ability of the ARB to relocate its readers should allow it to eliminate quickly any chance

---

[2] Afternote to 47 CFR 15.247. This admonition was apparently added to address concerns expressed by the National Telecommunications Information Administration (NTIA) that spread spectrum transmissions might interfere with government and military radio usage, which is the area regulated by the NTIA.

[3] Telephone interview with David Means, FCC Authorization and Evaluation Division Laboratory, Columbia MD, (301) 725-1585, ext. 206; May 17, 1993.

interference that might occur.[4] The FCC has also noted that any such interference would be extremely difficult to detect.

GM Hughes has conducted extensive field trials of the prototype system and found no serious interference problems. The most notable form of interference, with cellular telephones on vehicles, will be addressed by horizontal polarization of the transponder antenna, thereby minimizing interference with vertically polarized telephone antennas. Testing has been limited to use of the reader as a stationary roadside unit. The potential for interference if the reader is used in a roving mobile unit has not, to our knowledge, been explored. However, based on the considerations discussed above, interference with other licensed transmissions due to mobile operation is not expected to be a significant problem.

According to the FCC, use of spread spectrum technology has not caused interference problems to date, with one exception. The exception pertains to Automatic Vehicle Monitoring (AVM) broadcasts. AVM is a newer licensed two-way technology (up to 300 watts power) that is used to locate and communicate with vehicles; its primary use currently is for communications with commercial vehicles to locate cargo. AVM technology, under its official new FCC name of Location and Monitoring Service (LMS), is being considered for many other uses, including personal locators, navigation, safety, and Intelligent Vehicle Highway Systems (IVHS). IVHS use includes traffic congestion management, which is expected to include many of the transportation control measures required under federal and state clean air laws. Under FCC regulations proposed in response to a petition from Pactel Teletrac (58 FR 21276-21277, April 20, 1993; often referred to as the "Teletrac Proceeding"), the FCC has slotted LMS transmissions to occupy the 902-928 MHz band. The issue of spread spectrum transmissions causing interference with LMS has specifically been flagged in the FCC proposal:

> Some LMS systems have already experienced interference from Part 15 [unlicensed] devices. This will likely be a continual concern as new consumer-oriented Part 15 devices, including the new spread spectrum cordless telephones, which can operate with up to one watt, are introduced. (FCC Notice of Proposed Rulemaking, PR Docket No. 93-61, adopted March 11, 1993; FCC 93-141, at p.6)

The FCC proposal goes on to address the issue by suggesting an alert or warning be issued to LMS users. But perhaps the most significant statement in the FCC proposal is the following:

> LMS licensees could require some time to identify a source of interference and take action to eliminate the problem. As LMS systems are being marketed to public safety entities such as police and ambulance services, this potential interference is of special concern. We request comment from LMS operators

---

[4] Although primarily intended to operate as a stationary roadside unit, the GM Hughes reader is a portable, battery-powered device that can easily be moved from one operating site to another.

regarding measures that should be taken to protect against potentially life-threatening failures of LMS systems due to interference from other, lower priority users of the band. (Ibid.)

One commenter in the Teletrac rulemaking, Cylink, has suggested that the FCC should accord greater rights to Part 15 unlicensed users. If the FCC adopts this view, the ARB system would probably be protected. But the FCC could decide that restricting, rather than protecting, unlicensed users is the preferred approach. A decision by the FCC is expected by the end of this year.

According to GM Hughes, the prototype spread spectrum system is designed to mitigate this kind of interference, and actual interference is not expected to occur beyond a distance of about 50 feet. Nevertheless, interference could occur each time a LMS-transmitting or receiving vehicle passes near an ARB roadside reader unit (or possibly a vehicle transponder unit as well) that is simultaneously transmitting on the same frequency. This is an area of potential conflict that will have to be monitored by ARB.

If production transponder and reader units are upgraded to 100 milliwatts to 4 watts and converted from spread spectrum signals to a coherent signal at 915 MHz, the potential for interference with LMS transmissions (and other higher priority transmissions) may be increased due to higher transmitting power and loss of the ability to transmit on different frequencies. In addition, each reader unit will have to be licensed by the FCC, which opens up the possibility of the interference issue being raised by the FCC or an outside party as an objection to licensing. GM Hughes believes that any interference with LMS signals generated by a 4 watt unit would be brief and geographically confined enough such that actual disruption would not occur; CRC technology built into LMS systems, for example, should be able to overcome any minor interference that might occur. Nevertheless, it would seem advisable to undertake a thorough evaluation of the risk of interference with other signals, and to make direct contacts with the FCC, prior to making a commitment to upgrade the system as proposed.

Another possible source of conflict arises in connection with California's automated toll collection system. CalTrans recently issued uniform regulations governing two-way automated toll collection systems in the state based on transponder transmissions between vehicles and toll booths in the frequency band of 915±13 MHz, which would overlap the band where the ARB transponder system would operate.[5] GM Hughes indicates that the ARB system operates in a sufficiently different

---

[5] See new Articles 1-4 in Chapter 16 of Title 21, Code of California Regulations. CalTrans was given authority to set state-wide specifications and standards for automatic vehicle identification systems used by all toll collection operators in the state by SB 1523, which was passed in 1989 and codified as Streets and Highways Code Sections 27564 and 27565. Because no equipment is currently available to meet CalTrans requirements, the regulations contain a five-year "exemption."

manner such that its transmissions cannot interfere with CalTrans' system; likewise, CalTrans' system will be able to put an ARB transponder on alert, but will not trigger data transmission, when a vehicle is within 10 feet of a tollbooth. CalTrans has also expressed an interest in coordinating its system with the ARB system, as well as with other systems under consideration by the California Highway Patrol and the Department of Motor Vehicles, and has suggested the use of a single transponder unit that can transmit different data streams and be accessed by several agencies.[6] Coordination with CalTrans' system, and possibly with other agencies' systems, may require use of a different RF technology than that being currently developed for ARB by GM Hughes. Also, as discussed below, multiagency access to vehicles may raise additional Fourth Amendment privacy concerns.

The discussion above addresses mainly the problem of interference with higher priority transmissions caused by an ARB transponder program. The other form of interference would be where a stronger external signal disrupts transmissions from an ARB reader or transponder unit. According to GM Hughes, the prototype spread spectrum equipment proposed for the ARB program is relatively "immune" to higher power signals; such signals are coherent rather than spread spectrum, and the spread spectrum system has the capability of working around any such interference by changing codes, switching frequencies and resending the message if a signal corruption is detected by CRC. GM Hughes has not observed problems of this nature in its field testing. If production reader units are upgraded to 4 watt coherent signal units, interference from other signals may become a more significant issue. ARB should therefore require thorough field testing of such units before making a commitment to using them.

> RECOMMENDATIONS: ARB should follow the FCC proceedings on LMS transmissions to be sure that no decision is made that is adverse to the type of equipment proposed for use in the transponder program (both prototype and production). Prior to any upgrade of the reader unit to transmit a coherent signal at 4 watts of power, the FCC should be contacted to confirm the feasibility of licensing. Field testing to look for interference by other stronger signals should also be undertaken. Confirmation that there will be no significant interference with CalTrans tollbooth signals should also be obtained from CalTrans, and the opportunity for coordination with CalTrans, CHP and DMV systems should be explored. ARB should work with its equipment vendors to develop internal guidelines on use of transponder equipment, such as location, time of day, portability, etc., that will minimize the chance of interference with licensed transmissions.

---

[6] The CalTrans contact is Les Kubel, Chief of the Office of Electrical and Electronic Engineering, CALNET # 497-2405.

Liability

Overview – It is difficult to predict every avenue of liability that might result from a transponder program. In general, the potential hazards associated with transmitters would include property damage, personal injury or death resulting from:

- Interference with another electronic device on the vehicle (e.g., engine computer, speedometer, carphone or radio);

- Interference with an external electronic device or transmission, such as a traffic light radio signal, emergency vehicle transmission, or other higher priority licensed signal; or

- Distraction of drivers by monitoring equipment or activities contiguous to the roadside.

However, it does not appear that use of GM Hughes transponder technology in the manner proposed will actually create substantial risks in any of these categories. Extensive field testing indicates that transponder signals will not interfere with vehicle equipment, and roadside activities should not be more distracting than other kinds of activities presently encountered along the state's streets and highways. The only concrete form of risk, as discussed above, would be injury caused by interference with some critical external signal, such as a police, traffic, medical or aviation signal, and even that risk appears low based on GM Hughes testing and statements from FCC staff. Liability to a commercial user of a licensed LSM system would also be conceivable, although the more likely remedy would be to merely eliminate the interference by relocating ARB equipment or implementing a technical solution. Overall, the potential for injury associated with the proposed system appears to be minimal.

Tort Claims Act – The low-risk nature of a transponder program is reinforced by the limited circumstances under which California law permits governmental agencies (and employees) to be held liable. Liability of state agencies begins with the proposition that the state is immune from liability except where immunity has been expressly waived by statute or constitutional provision. The California Tort Claims Act (Government Code Sections 810–895.8) is the primary statute of interest.[7] The principal basis for any liability under the Tort Claims Act in this case would be negligence, i.e., a claim asserting that the failure of ARB or its employees to exercise due care caused injury to a person or property to which ARB or its employees had a legal duty to use due care. This is not a strict liability standard; the mere causation of injury will not necessarily result in liability. There must be a showing that ARB had the requisite duty and failed to act reasonably

---

[7] For a comprehensive discussion of the California Tort Claims Act, see "California Government Tort Liability Practice", Third Edition, California Continuing Education of the Bar, Berkeley, CA, 1992.

under the circumstances.[8] If ARB uses its public hearing process preceding the adoption of a transponder program to consider and act on any safety concerns, a strong reasonableness defense will be created. Compliance with all FCC requirements would also help demonstrate due care.

Further, there are several immunities that appear to be applicable. Under the Tort Claims Act, immunities prevent liability even where negligence may exist. Sections 818.2 and 821 of the Tort Claims Act provide that state agencies and employees are not liable for an injury caused "by adopting ... an enactment." This immunity, known as the legislative immunity, applies to the adoption of rules and regulations. Assuming ARB would impose a transponder requirement by amending its OBD regulations in Title 13, Code of California Regulations, this immunity would be directly applicable.

A second form of immunity is contained in Sections 818.4 and 821.2 of the Tort Claims Act, where public agencies and employees, respectively, are insulated from injuries resulting from the issuance or denial of a permit, license or certificate. This immunity could protect ARB from liability for certifying vehicles as in compliance with its transponder regulations. However, an important limitation is that this immunity only applies where the agency "is authorized by enactment to determine whether or not such authorization should be issued", i.e., where the decision is discretionary and not merely ministerial. It is not clear whether a court would view the ARB certification process as discretionary or ministerial, but a good case can be made that enough judgement is involved in the certification process to make it discretionary.

> RECOMMENDATION: ARB regulations should require vehicle manufacturers to certify that the transponder will not adversely affect the safety of vehicle operators, passengers or equipment, or persons or equipment external to the vehicle, under normal use conditions. Manufacturers should also be required to provide specified information regarding transponder safety; for example, by submitting test results (or at least a statement) indicating that interference with any standard or optional onboard electronic equipment will not occur. We also recommend that the regulation be stated, to the extent feasible, as a performance standard. For example, the regulation could simply state that the device must be capable of sending and receiving a specified kind of signal, and leave to the manufacturer the task of determining the design and placement of the transponder. This approach would tend to transfer any responsibility to vehicle manufacturers, who are in the best position to address such decisions, and also help characterize the certification process as discretionary rather than ministerial.

---

[8] The fact that transponders are operating within FCC-approved limits would be strong and possibly convincing evidence of due care in a case alleging liability caused by interference with an external signal.

Civil Rights Claim - There is one additional potential source of liability: a claim under the Federal Civil Rights Act (42 U.S.C. Section 1983). Section 1983 makes persons who are acting under color of any state law or regulation liable for injury caused by depriving another person of his or her federal constitutional "rights, privileges or immunities." Section 1983 also provides for equitable relief, such as injunction. It is possible that a claim could be filed under the Civil Rights Act by a person who believes that unconsented surveillance of a vehicle emissions control system by means of a transponder device violates his or her Fourth Amendment right to be free from unreasonable searches and seizures, or some other constitutional right such as the right to privacy. The risk of liability under Section 1983 is difficult to assess but is probably fairly low; the discussion of constitutional issues below provides some insight into the kinds of risks involved.

A critical feature of Section 1983 actions is that they may not be brought against the state itself or against state employees acting in their official capacity[9], but they may be brought against a state employee individually for actions taken while implementing a state law or regulation. Thus, ARB board members and staff are at risk, rather than ARB itself. Since Section 1983 operates as a basis for liability separate from the California Tort Claims Act, none of the limitations or immunities in that act can be used defensively. However, federal law does recognize a "qualified immunity" for state government officials who are not violating "clearly established statutory or constitutional rights that a reasonable person would have known."[10] This immunity may protect ARB members and employees because there are no clearly established rules prohibiting transponder surveillance of vehicles; in fact, as explained below under the analysis of Fourth Amendment issues, requiring transponders may well be constitutionally permissible.

Constitutional Issues

Introduction - There are two primary approaches to the use of transponder technology to read vehicle OBD codes: as part of the regular inspection procedure at licensed smog inspection stations, or as a separate program covering vehicles while they travel on public streets and highways. The question addressed here is whether either approach imposes an unjustifiable intrusion or imposition on individual Constitutional rights.

Because questions of constitutional rights are often involved, electronic surveillance by government has always been subject to close review by the courts, and court-ordered restrictions are often applicable. Constitutional law, which applies broad, fundamental tenets of governance to specific situations, and often involves unpredictable

---

[9] This prohibition is based on the 11th Amendment, which bars federal suits by private parties seeking to impose liability that would be paid out of state treasury funds.

[10] Harlow v. Fitzgerald, (1982) 457 U.S. 800.

"balancing" of competing interests or vague tests of "reasonableness", does not lend itself to mechanistic analysis and predictive certainty. This section will hopefully alert ARB to certain features of the transponder program that might encounter difficulty if subjected to court review, or that might cause public or legislative disfavor.

Use At Smog Check Stations - In the case of transponder use during smog inspections required on fixed occasions (biennially and on transfer of ownership or initial registration) at fixed sites (licensed Smog Check stations) by licensed inspectors, constitutional rights are not expected to be of direct concern. A vehicle would enter or pass by a test lane, where, instead of taking the time to physically connect the BAR analyzer to a data transfer port on the OBD system, the inspector would merely send a radio signal to activate the transponder and receive a radio transmission containing information stored in the OBD system memory. That information would tell the inspector whether fault codes existed, and also possibly what those codes are. The presence or absence of fault codes, or the nature of the code, could then be used to help determine what inspection or test procedures to run while the vehicle is at the station (e.g., an EGR fault code might trigger a specific functional check, or the absence of any fault codes might allow a shortened test procedure). A fault code could also be used to help generate a recommended diagnosis or repair in the case of failed vehicles, and thereby reduce errors in vehicle problem diagnosis.

From a legal viewpoint, the key factors are that automated retrieval of OBD data is occurring with the vehicle owner's knowledge (and with the owner's actual or implied consent), at a fixed station, under a set procedure, by a qualified person who applies the procedure in the same manner to all vehicles with equal frequency. Under these circumstances, transponder technology is being used only as a modification to the established inspection and test procedure to improve its accuracy and efficiency. The information obtained relates primarily to vehicle emissions components; the transponder is not being used to obtain personal information about vehicle owners or drivers. There is no added element of surprise, either as to the requirement for an inspection or the scope of the inspection. Transponder technology is being used to obtain the same information that would be obtained under the current program with scan tools that physically connect to the vehicle, only with greater efficiency and accuracy.

The U.S. Supreme Court has made it clear that it is permissible for states to conduct inspections of vehicles for valid safety and other regulatory purposes, where the inspection does not involve random stopping of vehicles or other procedures that give state officials "standardless and unconstrained discretion" or unduly threaten vehicle owners. See, for example, Delaware v. Prouse, 440 U.S. 648 (1979) (court banned completely random stopping of vehicles by police to inspect licenses); U.S. v. Martinez-Fuerte, 428 U.S. 543 (1976) (allowing stopping of vehicles at fixed stations near the border to inspect for customs and immigration violations); and Michigan St. Police Dept. v. Sitz, 496 U.S. 444 (1990) (allowing roadblocks to stop all vehicles and inspect drivers for signs of intoxication). Periodic inspection of vehicles at licensed Smog Check stations would appear to fall well within the scope of these cases, and modifying the Smog Check

station inspection procedure to provide for transponder data acquisition does not add any new threat to personal rights.

On-the-Road Use of Transponders - Application of transponder technology to obtain information from vehicles as they travel on the road is another matter. In the on-the-road scenario, the transponder on the vehicle would be activated by a signal from a roadside reader as the vehicle is moving along the roadway. Once the two devices have a confirmed link, data would be transferred from the vehicle to the roadside reader. The data would consist of the VIN (Vehicle Identification Number) and certain information stored in the OBD system of the vehicle. The whole process would take place in milliseconds. No advance notice would be given to the motorist. No stopping of the vehicle would occur, and unless the system had a built-in activation alert (or the driver happened to see and recognize the roadside reader unit), the driver of the vehicle would be completely unaware that surveillance of his or her vehicle had just occurred. An illuminated malfunction indicator light on the vehicle dash might warn the driver that the vehicle would provide a fault code if probed by radio, but would not provide an actual warning of a remote access event.

The data from such a program could be used simply for research purposes; for example, to help monitor effectiveness of the regular I/M program or OBD systems. However, the data could be used to implement an automated enforcement procedure. The simplest approach would be for the transponder information to be screened by ARB within several weeks after acquisition. Correction notices would then be sent by mail to owners of vehicles with valid readings of fault codes. The notices would require an out-of-cycle certificate of compliance from a Smog Check station to obtained within a specified time period, e.g., 30 days. A record of the notice would be sent to DMV, and DMV would withhold re-registration of the vehicle at the next annual re-registration date unless a certificate of compliance covering the transponder incident accompanied the application for re-registration. A monetary penalty for failure to obtain the out-of-cycle certificate of compliance in a timely fashion could also be imposed, either through DMV or by forwarding notices to local courts if a certificate of compliance were not sent to ARB within 30 days (like a parking ticket).

More aggressive enforcement techniques would also be available. If data from a vehicle indicate that a fault code has been stored, that information, along with identification of the vehicle from its VIN, could be relayed to a CHP/ARB roadside team further down the road on a real-time basis. The team could then stop the vehicle and issue a correction notice requiring an out-of-cycle smog check. The roadside team could issue the correction notice based on the transponder reading alone, or conduct a confirmatory underhood inspection of the vehicle on the spot. The inspection could be further expanded to include a tailpipe emissions test.

From an emissions control perspective, on-the-road surveillance of OBD information has definite advantages. If a vehicle has a malfunctioning emissions component, a network of transponder readers, possibly including roving mobile readers, operating on a regular basis on major urban thoroughfares will provide a means for detection and repair within

a matter of days or weeks for many vehicles. Under the current biennial program, it could take up to two years for the malfunction to be detected and repaired. The potential emission benefits of a transponder program will be addressed in a subsequent report by Sierra.

However, use of transponder technology in on-the-road applications, such as those described, would introduce a number of new program elements, not present in the existing fixed-station I/M program, that raise Constitutional questions:[11]

- Motorists will typically not be informed before monitoring takes place.
- Motorists will not know that a surveillance has occurred (except through receipt of a correction notice after a fault code has been recorded).
- Vehicle owners may have no opportunity to monitor or record conditions during a surveillance, or to have a contemporaneous confirmatory test done by a Smog Check station, and thus will be precluded from obtaining information that might be used to rebut a claim of violation by the government.
- There will be no restriction on the number of times a vehicle is monitored, or on the frequency of surveillance; some vehicles will be monitored frequently, others hardly at all, depending on the routes they are driven.
- More frequent detection of OBD fault codes could result in more frequent inspection and repair obligations, and thus greater cost and inconvenience to motorists.
- Whether used or not for this purpose, reading the VIN will allow transponder equipment to monitor the whereabouts of specific vehicles.

---

[11] These questions also raise public policy issues that could be controversial and arouse the interest of special interest groups and the state Legislature. An informal poll of Sierra employees, taken during the course of preparing this report, resulted in a large majority not favoring electronic monitoring. Last year the Legislature passed SB 1447, which amended CalTrans' authority to establish an automated vehicle identification system for tollbooths to give motorists "the option of using the automatic toll collection system with a passenger vehicle in a manner that does not identify the user, vehicle operator, vehicle owner, or vehicle at the time the occupant pays the tolls or lawfully uses the facility." SB 1447 was vetoed by the Governor. If this provision had been enacted into law, it would have effectively eliminated CalTrans' ability to implement an enforceable toll collection program. If a similar prohibition were imposed on the ARB transponder program, it would have the same effect, and limit the program to data gathering.

- The same system could be expanded to gather other data such as maximum speed, total time in excess of a given speed, mileage, and route information; to monitor the condition of certain safety-related equipment such as tires and brakes; and to collect roadway use fees.

- The emission benefits of the program in some cases may be limited due to poor correspondence between fault codes and actual defects in emission control equipment or actual excess emissions.

Fourth Amendment - Search and Seizure. The Fourth Amendment to the U.S. Constitution states:

> "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated...".

Identical language appears in Article I, Section 19, of the California Constitution.

It is well established that the Fourth Amendment applies to vehicles, even though vehicles are not specifically mentioned in the language of the amendment. However, the U.S. Supreme Court has made it clear that vehicles are subject to a "diminished expectation of privacy" compared to a residence or personal effects. (See U.S. v. Knotts, 460 U.S. 276 (1983), where the Supreme Court allowed police to monitor the location of a vehicle by hiding an electronic beeper in a drug container carried in the vehicle; New York v. Class, 475 U.S. 106 (1986), where the Supreme Court allowed police, without cause or issuance of a warrant, to examine the vehicle identification number (VIN) of vehicles on the street; and California v. Carney, 471 U.S. 386 (1985), where the court allowed a warrantless inspection of a mobile home.) In the Carney case, the court noted that the "automobile exception" to the right to privacy derived from the need to allow greater latitude for government inspection due to both the "mobility" of automobiles as well as the "pervasive regulation of automobiles." This exception is especially relevant to the ARB program, because the ARB is seeking information about the vehicle, and not about the person owning or driving the vehicle.

With this diminished expectation of privacy in mind, a number of constitutional law treatises and U.S. Supreme Court cases on Fourth Amendment rights were reviewed. One basic conclusion stands out: where there is no physical trespass of a person's property, technologically enhanced governmental surveillance will usually be allowed. Or, as recently stated by a 9th Circuit District Court:

> Time and again, the United States Supreme Court has held that police utilization of extra-sensory, non-intrusive equipment...to investigate people and objects does not constitute a search for the purposes of the Fourth Amendment. (U.S. v. Penney-Feeney, 773 FS 220 (1991), allowing police to use an infrared detector device to read the heat signature of

a residence where operation of a marijuana hothouse was suspected.)[12]

Use of transponder technology to obtain remote readings of the condition of vehicle emission control systems would clearly fall within this category of "non-intrusive" investigations.

In deciding such cases, the Supreme Court uses a sequence of two questions: 1) Did the conduct of the individual exhibit an actual expectation of privacy? and 2) Was the individual's expectation of privacy one that society is prepared to recognize as reasonable? (first iterated in Katz v. United States, 389 U.S. 347 (1967)). Under this approach, the court has allowed numerous kinds of non-intrusive technology-enhanced searches to take place, including monitoring vehicle movement by means of an electronic beeper (United States v. Knotts, 460 U.S. 276 (1983)), aerial surveillance of private property (California v. Ciraolo, 476 U.S. 207 (1986) and Florida v. Riley, 488 U.S. 445 (1989)), and use of a "pin register" to record numbers called from a private telephone (Smith v. Maryland, 442 U.S. 735 (1979)). Most of these cases have been disposed of under the first question, i.e., by determining that the individual did not have an actual expectation of privacy. In the Knotts case, for example, the court concluded that a person cannot expect to keep the movements of a vehicle private when it is driven on public streets, and that the beeper merely augmented the ability of drug enforcement officers to follow the vehicle visually.

Assuming that the approach used by the Supreme Court in these cases would be governing in any constitutional challenge to a transponder program, there is some assurance that a transponder program would pass constitutional muster. The answer to the first question in the Katz test should be in the negative — i.e., no expectation of privacy would be found. Since the surveillance applies to vehicles, a reduced expectation of privacy would be applicable in the first instance under the cases cited previously. Moreover, as transponder technology will not enable the state to obtain more information than it would otherwise be able legitimately to obtain by simply increasing the frequency or scope of the current fixed-station I/M program, no unique invasion is being created. It would be very difficult for a California motorist to establish an actual expectation of privacy as to the condition of his or

---

[12] Also see Rotunda and Nowak, "Treatise on Constitutional Law", 2d Ed., West Publishing Co., 1992, at pages 372-382. The authors' main conclusions are that "The Supreme Court has not yet held that the right to privacy limits governmental powers relating to the collection of data concerning private individuals." (at page 372), and that the Supreme Court has "narrowed" the Fourth Amendment right of privacy only to cases where individuals have a "legitimate expectation of privacy" strong enough to be analogous to a "legally cognizable property right" (at page 379, fn. 74).

her vehicle's emission control system given the pervasive vehicle emission regulatory program in the state.[13]

Even if the first question is answered in the affirmative, there is a likelihood that the second would not. California's air pollution problems are recognized as the worst in the nation, and the contribution of vehicle emissions to that problem have earned California the unique right to establish its own vehicle emission control program under a waiver of federal preemption in the federal Clean Air Act (42 U.S.C. 7543). Similar recognition of the need for special efforts to control vehicle emissions is contained in state law (see Part 5 (commencing with Section 43000) of Division 26 of the Health & Safety Code). Under these conditions, a court may well find that there is an overriding societal interest in clean air.

However, there is one important caveat as to the applicability of these cases: in each case, surveillance was initiated on the basis of pre-existing suspicion of an individual or small group of individuals, whereas the transponder program would apply to motorists at large. The cited cases are factually the most closely allied that could be found among those decided by the Supreme Court, but Sierra could not identify any Fourth Amendment cases involving mass surveillance. By proposing a program involving suspicionless electronic surveillance of a large number of citizens, the ARB appears to be opening the door to a broader use of technology than has been reviewed by the Supreme Court to date. Thus, constitutional review of a transponder program would involve novel circumstances, and a novel set of decisional factors could evolve. It is possible that the court would use a different, less permissive test where information is electronically obtained without prior suspicion.

There is another important aspect of the transponder program that could become an overriding factor. If owners of vehicles with on-board transponders are informed in advance of the presence of the device and how it will operate through an appropriate admonition in the owner's manual, DMV registration or licensing procedures, or through other consumer information, the defense of actual or constructive consent would be raised. If consent is found, Fourth Amendment claims would be avoided altogether.[14]

The primary public concern about a transponder program may, in fact, not be its use to monitor the status of vehicle emissions control equipment,

---

[13] The fact that all emission data are viewed as public information under the California Public Records Act (Government Code §§ 6250 et seq.), while not directly applicable, would help support this position.

[14] In United States v. Karo, 468 U.S. 705 (1984), the Supreme Court explicitly decided that neither the secret installation of an electronic beeper in a canister of drugs prior to delivery to a buyer, nor the subsequent transfer of the canister to the buyer without informing him of the beeper, constituted a "search or seizure" under the Fourth Amendment. It is uncertain whether the same ruling would result in the case of a transponder installed without informing the vehicle owner and without prior cause or suspicion of the vehicle owner.

but rather its introduction of a technology with the potential to monitor many other aspects of vehicular travel. As noted above, a number of other state agencies have expressed an interest in using the same technology, including CalTrans, the CHP and the DMV. Expansion of the system to access data on vehicle speed, mileage, passenger load, weight, safety equipment, registration date, etc., would be useful to these agencies. We have already noted CalTrans' new regulations to collect tolls by means of transponder signals. The ARB itself might want to explore expanded use of transponders to implement or enforce certain traffic control measures for emission reduction purposes. The same transponder data that are gathered for emissions purposes would, in the hands of a criminal investigative agency, enable that agency to determine whether a particular vehicle has passed by certain checkpoints on a daily basis; by the simple expedient of acquiring a few mobile reader units, an investigative agency would have access to technology that would be able constantly to monitor the vehicular movements of selected individuals along any number of routes, or readily locate vehicles. To some, these uses would appear Orwellian.

In the Knotts case cited above, the Supreme Court specifically considered and rejected the claim that allowing surreptitious use of electronic beepers would make possible "twenty-four hour surveillance of any citizen of this country...without judicial knowledge or supervision." While acknowledging the possibility of such use, the court said that "reality hardly suggests abuse", and that "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough to determine whether different constitutional principles may be applicable" (460 U.S. at pp. 284 and 285).[15] Since the ARB transponder program, by itself, would not involve such expansive surveillance, the mere potential for creation of a larger program through coordination with other agencies would not appear to create additional risks. However, ARB should evaluate such risks before linking its system to uses sought by CalTrans, CHP, DMV or any investigative agency. While the views expressed in the Knotts case seem dispositive, the court could distinguish the Knotts case as one involving a search and seizure based on cause or prior suspicion, and apply a more restrictive rule in the case of a transponder program applied broadly to suspicionless persons.

In order to maintain public support for its program, Sierra believes that ARB should be mindful of the legal uncertainties associated with expanded use of transponder technology, and consider steps to limit use of transponder equipment and data by ARB employees and other governmental agencies. Although not yet required by the Supreme Court, such limitations have been mentioned as critical in a number of concurring or minority opinions, which could someday become a majority

---

[15] This is consistent with the Supreme Court's rule that it will not rule on facts or issues not actually before it. Also see Whalen v. Roe, 429 U.S. 589 (1977) where the court noted that the "mere possibility" that personal data on prescription drug use would be used improperly did not invalidate a law requiring pharmacists and doctors to provide copies of prescriptions containing certain narcotics.

position.[16] Such limitations may also help prevent harsh legislative oversight and reaction.

A final question is whether the Fourth Amendment principles discussed above might apply differentially if the program is conducted purely for the purpose of research or data-gathering, with no application of sanctions against motorists. Sierra could locate no directly applicable court rulings. The Fourth Amendment is mainly raised as a defense by criminal defendants, and the reported cases thus involve criminal sanctions. However, by its own terms, the Fourth Amendment comes into play whenever the government conducts an unreasonable search or seizure, and does not require application of criminal or other sanctions. A "search" would almost certainly be found when transponder data is accessed. So it is likely that a research-based transponder program would trigger Fourth Amendment protection. The issue then becomes whether limiting use of transponder data to non-enforcement purposes affects the determination of whether a search is reasonable. As noted in the previous paragraph, some members of the Supreme Court have viewed how data are used as a relevant factor, so it is possible that the court would allow a search for data-gathering purposes but disallow the same search if information obtained in the search can lead to sanctions.

If the program is expanded to include stops by on-the-road inspection teams, an intrusive element is added. However, as long as the initial electronic data access is ruled reasonable and the subsequent inspection portion of program meets the requirements announced by the Supreme Court in its roadblock cases, cited above, there should be no Fourth Amendment infirmity. Because an inspection team will stop only vehicles with emissions-related OBD fault codes, the prohibition against random stops will not be applicable. A team will also be using specific inspection procedures and calibrated equipment, and thus will not be exercising "standardless and unconstrained discretion." If there is one area of concern, it would be the scope or duration of the inspection. It is possible that a court would rule an on-the-road inspection unreasonable if the procedure is too detailed (e.g., involving disconnection of the evaporative system or tailpipe measurements at various engine RPMs) or takes too long to complete.[17]

---

[16] See, for example, Justice Brennan's concurring opinion in Whalen v. Roe, 429 U.S. 589, at pp. 606-607.

[17] ARB is currently conducting roadside snap-idle and inspection tests on commercial heavy-duty Diesel vehicles when they stop at CHP weigh stations. The tests take several minutes to complete. In the context of highly regulated commercial vehicles, already stopped for other purposes, an additional stop of several minutes duration may be reasonable. See Michigan v. Sitz, 496 U.S. at 454, where the court noted that trucks may be subject to "further detention" for safety and regulatory inspection at roadside weigh stations. But stopping a private citizen driving his or her personal light-duty vehicle on personal business may be viewed as a more sensitive intrusion. In Michigan v. Sitz, for example, the court noted that "Detention of particular motorists for more extensive field sobriety testing may

(continued...)

RECOMMENDATIONS: To assure the integrity of a transponder program under the Fourth Amendment, ARB should consider implementing the following safeguards:

1. Consent - By regulation, ARB should require manufacturers to inform vehicle owners in the owners' manual and in a consumer notice provided at the time of first sale that a vehicle has a transponder on board and that by purchasing the vehicle they are consenting to emissions equipment surveillance by roadside units. The admonition might be worded as follows:

   This vehicle is equipped with an electronic transponder unit. When signaled by a roadside reader, this unit will send data from the vehicle's on-board emission monitoring system identifying the vehicle and indicating whether any emission control equipment has malfunctioned (or been tampered) and is in need of repair. The transponder unit may be signaled to send such data at any time while it is being driven on public streets or highways. BY PURCHASING OR USING THIS VEHICLE, YOU ARE CONSENTING TO THE TRANSMISSION OF SUCH EMISSIONS-RELATED INFORMATION.

2. Limitations On Use of Data - By regulation, ARB should require its staff to treat transponder data as confidential and, except for data required by court warrant, prohibit dissemination of such data to private persons. Transmission of ARB data to other agencies for official use could be allowed, if the agency provides similar confidentiality safeguards. Transponder equipment could also be programmed automatically to erase transmissions, including the VIN, if no fault code is received.

3. Other Safeguards - There are other measures available to address some of the issues noted earlier. The concern about secretly obtaining information could be addressed by having a light come on or beeper sound when a transponder is accessed by a reader, or even by providing a LCD readout to the driver of the nature of the fault, thus giving motorists the opportunity to run confirmatory tests or make early repairs. The Hughes prototype equipment already has indicators built in. Such measures would probably not reduce program effectiveness.

Right to Privacy - The U.S. Constitution does not explicitly refer to a right of privacy. Many Fourth Amendment cases speak of protecting individual privacy, but in such cases, the term seems to be used only as a shorthand reference to the right against unreasonable searches and seizures, and not a separate, independent right. The Supreme Court has recognized an independent right of privacy; however, it has been invoked only in certain limited circumstances involving "fundamental rights" or

---

[17](...continued)
require satisfaction of an individualized suspicion standard" (496 U.S. at 451).

highly personal areas, such as lifestyle, sexual activity and pregnancy[18]. In such cases, the Supreme Court typically determines that an independent right to privacy derives from the Fourth Amendment, as well as other constitutional rights such as the Fourteenth Amendment right to due process, an unenumerated right "retained by people" under the 9th Amendment, and as an element of "liberty" preserved by the Constitution. But, in general, the court has not been sympathetic to abstract privacy claims asserted in cases involving governmental access to data or information concerning individual citizens where an important or compelling public need for the data can be demonstrated.[19] In view of the reduced expectation of privacy criterion that has been applied to automobiles in the past by the Supreme Court in Fourth Amendment cases, we believe there is virtually no chance of the court striking down a transponder program as violative of an independent right to privacy.

In California, however, there definitely is an independent right to privacy. The California Constitution provides in Article I, Section 1, that

> All people are by nature free and independent, and have certain inalienable rights, among which are those of ... pursuing and obtaining safety, happiness and privacy. (Emphasis added; emphasized words added by Initiative in 1972)

This raises the question whether privacy, because it is an explicitly mentioned right in the state Constitution, enjoys a higher status in California. Two treatises examining this question have concluded that at least some degree of additional protection is afforded under the California Constitution, and possibly a great deal more protection.[20] As an example of the difference between federal and California law in this area, compare Valley Bank v. Superior Court, 542 P.2d 977 (1975), where the California Supreme Court decided that private bank records could not be discovered in a civil case, with U.S. v. Miller 425 U.S. 435 (1976), where the U.S. Supreme Court allowed the subpoena of private bank records in a criminal investigation. The different result in these two decisions may be explained by the fact that the former merely involved civil discovery, while the latter addressed a more important need for governmental information in a criminal case. Nevertheless, it appears that the explicit right to privacy in California will require a compelling justification for any intrusion occasioned by a transponder program, instead of the less onerous balancing or "reasonableness" approach used under the Fourth Amendment of the federal Constitution. A transponder program may, in fact, satisfy a constitutional test in California requiring a compelling public need, because it would contribute to reducing the state's serious air pollution problem.

---

[18] See, e.g., Griswold v. Connecticut, 381 U.S. 479 (1965) state prevented from regulating birth control in private homes); Roe v. Wade, 410 U.S. 113 (1973) preventing certain state regulation of abortion).

[19] See Rotunda and Nowak, cited in fn 6, at pp. 372-382.

[20] See 13 Cal Jur 3d at Sec. 237, and 19 Pepperdine Law Review 327, 329 (1992).

Due Process/Equal Protection - To meet the due process requirement of the Fourteenth Amendment to the U.S. Constitution, a government enactment must meet a basic "fairness" test (procedural due process) and be rationally related to a valid public purpose (substantive due process).[21] Equal protection under the Fourteenth Amendment to the U.S. Constitution likewise allows enactments that do not differentiate on the basis of "suspect" categories or that do not involve "fundamental" liberties, to treat categories of persons differently as long as there is a rational basis for differentiation.[22] Similar due process and equal protection requirements apply under Article 1, Section 7, of the California Constitution.

Readers in a transponder program will be located mostly in urban areas, and mostly on heavily travelled freeways and through streets. Persons who drive on such roads may have their vehicle monitored every day. In contrast, those who drive on side streets or in less populated areas may escape monitoring altogether. Urban drivers, whose vehicles are frequently monitored, may claim that the program is singling them out and, for that reason, discriminatory. Sierra does not believe that focusing the program where most vehicles travel will create a due process or equal protection constitutional infirmity. The "discrimination" in this case does not single out persons based on a suspect classification, and bears a rational relationship to the problem addressed, in that focusing on heavily travelled roads also focuses on the areas of greatest vehicular emissions.

ARB regulations will have to address the problem of a vehicle that regularly travels a frequently monitored roadway (e.g., the Santa Monica freeway in Los Angeles) on a daily basis, and that could receive repeated notices for the same equipment defect once its OBD system has stored a fault code. A data screening system will have to be put in place to prevent notices from going out for the same vehicle over a relatively short time frame (e.g., 60-90 days). If this is not done, we believe a court would question, under tenets of procedural due process, the fairness of the program.

Another potential problem relates to "false positive" OBD readings, i.e., issuing notices based on fault codes stored when there is no detectable or repairable defect in emissions equipment, when the defect is transitory or self-correcting, or when the defect does not cause a significant emissions increase. ARB's OBD II requirements are very extensive and require sensors to be highly sensitive to changes in emission-related operating parameters. "False positives" could result from a conservative design approach that results in a fault code being set when the vehicle is still meeting applicable standards, or from a fault caused by operation of a vehicle under abnormal conditions rather than an actual failure of an emission control system component.

If problems of this nature are pervasive, and result in too many vehicles being inspected with no defect being found, a transponder

---

[21] See Rotunda and Nowak, cited at fn 6, Vol. 2 at pp. 408-415.

[22] Ibid., Vol. 3 at pp. 20-28.

program could be subject to a due process challenge in court.[23] For such a challenge to succeed, it would have to be shown that the program is so flawed that it does not reasonably relate to the objective of reducing emissions from vehicles. Sierra does not believe ARB would face a high risk of losing such a case; the greater risk might be before the legislature. Nevertheless, we believe ARB should have confidence that the reliability and effectiveness of the transponder program, both in terms of avoiding false positives and having demonstrable emission benefits, is well established prior to public implementation.

RECOMMENDATIONS:

1. Screening Of Data - ARB regulations should include a procedure for screening of transponder data so that vehicle owners are not sent repeated notices for the same fault code. Setting a 60-90 day minimum limit between notices on the same vehicle would be one way to accomplish this. As noted above, an automated electronic screening technique could be used.

2. Reliability - Before the public is required to make repairs based on data obtained in a transponder program, ARB should review its OBD II regulations and conduct a pilot or experimental program to ascertain what fraction of the vehicle population will be receiving notices based on transponder data. The program should also examine the incidence of "false positives" and the ability of mechanics to find and repair defects flagged under the program. If necessary, changes to ARB OBD II regulations should be made.

Authority to Adopt

Introduction - A final issue is whether ARB has the authority under its current statutory delegation to implement a transponder program, or whether legislation is needed.

Sierra assumes that ARB would implement a transponder program by amending its OBD regulations (currently codified in Sections 1968 and 1968.1 in Title 13, California Code of Regulations) to add a requirement for vehicle manufacturers to install a transponder unit capable of reading, storing and transmitting certain OBD data, plus other information such as the VIN. The transmission requirement would include performance specifications that assure compatibility with ARB's roadside

---

[23] Any case challenging the transponder program on these grounds would also very likely claim that the regulation is invalid under Article 7 of the California Administrative Procedure Act (Government Code Sections 11350-11356) and/or a mandamus or administrative mandamus proceeding under Sections 1085 or 1094.5 of the California Code of Civil Procedure. These provisions require state agency regulations to be supported by "substantial evidence."

readers as well as compliance with FCC spread spectrum regulations. The regulations would also specify durability, certification and warranty requirements.

As currently written, the statutes relating to ARB regulatory powers do not specifically mention OBD systems or a transponder program. Thus ARB authority will have to be inferred from more general grants of legislative authority. Sierra has identified several areas, discussed below, where existing ARB authority could be interpreted to include authority to implement a transponder program.

Emission Standards - A number of sections in the Health & Safety Code direct ARB to adopt and enforce "emission standards" for motor vehicles.[24] Of particular relevance would be ARB's authority in Section 43101 to prescribe emission standards for the I/M program, since monitoring vehicles via transponder technology would operate like an expansion of the current I/M program. The term "emission standards" is defined in Section 39027 as "specified limitations on the discharge of air contaminants into the atmosphere". There is some question under this definition whether OBD and transponder requirements are an emission standard, but it is possible that a court could reach the conclusion that they are. ARB relied on its power to set emission standards as one of the sources for its authority to impose its OBD II requirements in 1990.

Test Procedures - It is possible to interpret ARB's OBD regulations as a form of "test procedure" for determining compliance with its emission standards. See Sections 43102 and 43104. This authority was also cited by ARB in support of its OBD II regulations in 1990.

In-Use Performance Standards - Section 43013 authorizes ARB to adopt motor vehicle "in use performance standards" which are "necessary, cost-effective, and technologically feasible to carry out the purposes of this division." This broad grant appears to fit an OBD-based transponder program better than the term "emission standards", in that the program is, in fact, designed to assure proper performance of in-use vehicles. This section was also cited by ARB in adopting its OBD II regulations.

"Whatever Actions Are Necessary...." - Sierra believes Section 43018 contains ARB's strongest legislative authority for a transponder program. This section, in relevant part, states:

> (a) The state board shall endeavor to achieve the maximum degree of emission reduction possible from vehicular and other mobile sources in order to accomplish the attainment of the state standards at the earliest practicable date.
>
> (b) Not later than January 1, 1992, the state board shall take whatever actions are necessary, cost-effective, and technologically feasible in order to achieve, not later than December 31, 2000, a

---

[24] See, for example, Sections 43000, 43010, 43101, 43102, 43104. All subsequent code references are to the Health & Safety Code unless otherwise indicated.

reduction in the actual emissions of reactive organic gases of at least 55%, a reduction in emissions of oxides of nitrogen of at least 15 percent from motor vehicles... The state board shall also take action to achieve the maximum feasible reduction in particulates, carbon monoxide, and toxic air contaminants from vehicular sources.

(c) In carrying out this section, the state board shall adopt standards and regulations which will result in the most cost-effective combination of control measures on all classes of motor vehicles and motor vehicle fuel, including, but not limited to, all of the following:

....

(2) Reductions in emissions from in-use emissions [sic] from motor vehicles through improvements in emission system durability and performance.

.... (Emphasis added)

This provision, with specific reference to emissions from in-use vehicles and emission system performance, gives ARB wide discretion to adopt regulations that will achieve the stated emission reductions from motor vehicles. A transponder program, assuming it meets the required necessity, cost-effectiveness and feasibility constraints, would be consistent with this mandate.

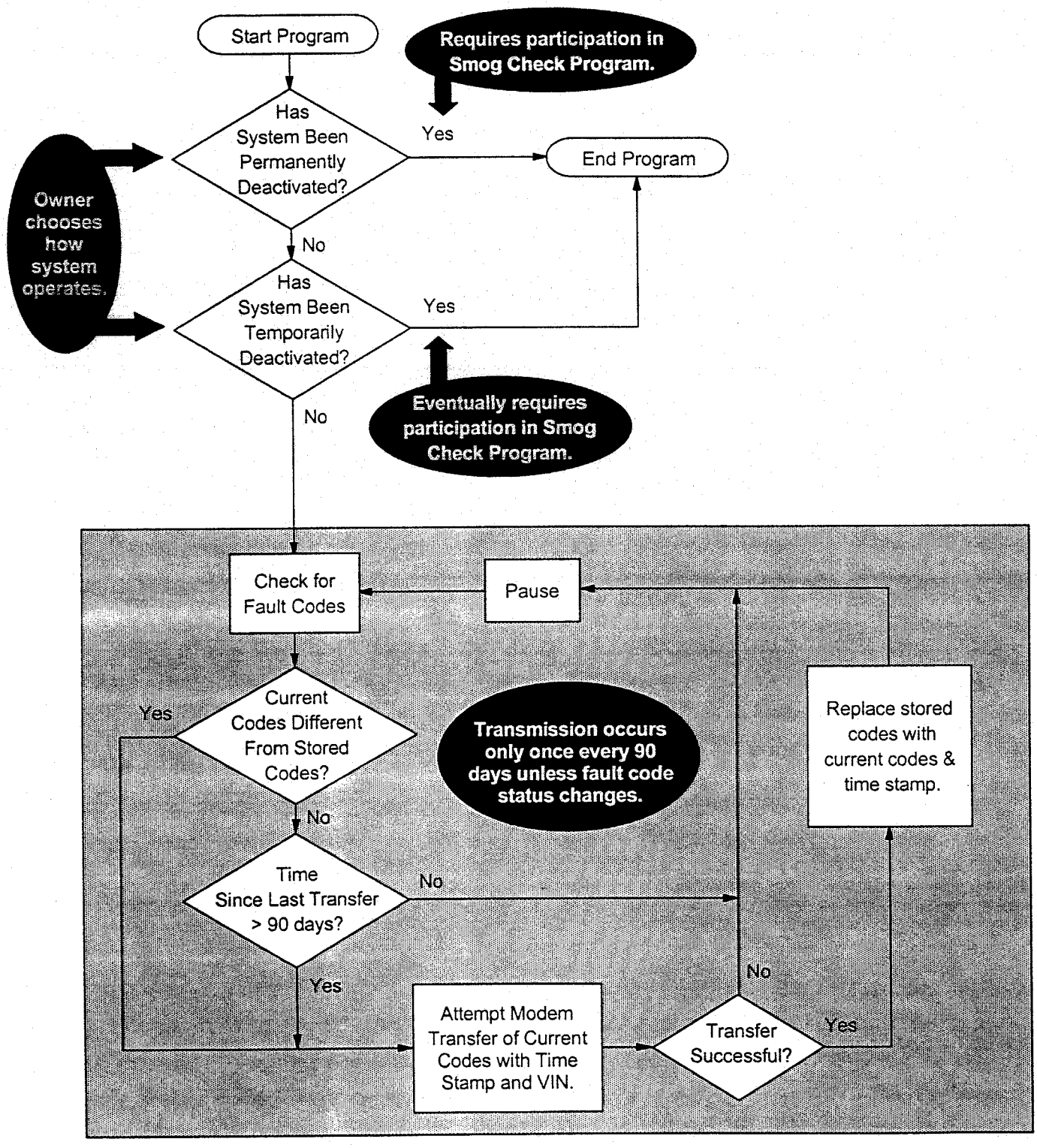
In lieu of relying on these existing statutory provisions, ARB could sponsor legislation granting it specific authority to implement a transponder program. The risk of such legislation being rejected or qualified in a manner unacceptable to ARB argues strongly against such an approach.[25]

RECOMMENDATION: ARB should rely on its existing statutory authority to implement any transponder program.

[25] In Clean Air Constituency v. California Air Resources Board, 11 Cal 3d 801 (1974), the California Supreme Court cited the failure of the Legislature to pass a number of bills proposing to give ARB explicit authority to delay the NOx retrofit program as one basis for concluding that ARB did not have the implied authority to institute such a delay.

Attachment B

Concept for OBD III System Operation



Sierra Research, Inc.

Attachment C

Privacy Principles for California

Draft* -- *for Discussion Purposes

Prepared for the Joint Legislative Task Force on Personal Information and Privacy
Senator Steve Peace, Chair
March 3, 1998

Beth Givens, Director Privacy Rights Clearinghouse	Telephone: (619) 298-3396 Fax: (619) 298-5681
1717 Kettner Ave. Suite 105 San Diego, CA 92101	E-mail: prc@privacyrights.org Web: www.privacyrights.org

Index:

Note: These principles were drafted for discussion purposes by the Joint Legislative Task Force. They were not adopted. -- *B. Givens*

Summary of Privacy Principles

Definition: The word "organization" is used broadly to also mean government agency, business, nonprofit, association, etc.

1. **Principle of proactivity.** Privacy implications are recognized explicitly and shall be considered when personally identifiable information is to be collected, accessed, stored, merged or otherwise manipulated, and when the application of any new information technology is introduced.

2. **Principle of secondary use.** Personal information shall not be used or disclosed for purposes other than those for which it was collected. Secondary use is permitted only with the affirmative consent of the individual.

3. **Principle of access.** An organization shall make specific information available to individuals about its policies and practices relating to the handling of personal information. Individuals shall have reasonable means to learn about, obtain and review, and when necessary, correct and amend information about themselves.

4. **Principle of affirmative consent.** The knowledge and consent of the individual are required for the collection, use or disclosure of personal information.

5. **Principle of relevance.** The collection of personal information shall be limited to that which is necessary for the transaction with the individual and purposes identified by the organization. The purpose for which personal information is collected should be specified at the time of collection. Personal information shall be retained only as long as

necessary for the fulfilment of those purposes.

6. **Principle of accuracy.** Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

7. **Principle of security.** Reasonable physical, technical and administrative safeguards will be taken to protect personal information against the risk of unauthorized access, collection, use, disclosure or disposal.

8. **Principle of accountability.** An organization is responsible for personal information under its control and shall designate a person who is accountable for the organization's compliance with the principles. A mechanism for oversight and enforcement shall be established to ensure the observance of these principles. An individual shall be able to challenge compliance with the above principles with the person who is accountable within the organization.

9. **Principle of progress.** As information technologies advance, privacy considerations are likely to change. The principles will be reviewed on a regular basis to ensure their adequacy.

* * * * * * * * * * * * * *

Analysis of Privacy Principles

Introduction

California is a uniquely privacy-conscious state. It is one of only ten states with a constitutional right to privacy. The constitutional provision not only prohibits the state from committing privacy intrusions, but also applies to the private sector as well (Article 1, Section 1, California Constitution, amended in 1972).

California has many privacy-related laws on the books. These address government agency information use, telephone records and wiretapping, credit reporting, telemarketing, medical records, employment records, cable television viewing patterns, video rental records, merchant information gathering, insurance record-keeping, and identity theft. In many instances, California has led the nation in the creation of such laws.

Californians themselves take extra steps to protect their privacy. For example, over 50% of households have unlisted telephone numbers. That figure reaches nearly 70% in Sacramento, San Diego, Los Angeles, San Jose, Fresno and Oakland. The national average, in contrast, is 24% of households. (Survey Sampling Inc., 1997)

The Privacy Rights Clearinghouse itself is uniquely Californian, the only program of its kind in the country. It was established with funding from the California Public Utilities Commission's Telecommunications Education Trust (TET), a grant program established in the late 1980s from a fine levied upon Pacific Bell for deceptive and abusive marketing practices. At the time, both the fine and the TET grant program were unprecedented in the nation. (The TET program ceased operation in 1995.)

California is also home to many high-tech companies that have pioneered privacy-enhancing technologies such as encryption. These companies continue to lead the world in developing a broad range of software products that enable individuals, corporations and government agencies to safeguard personally identifiable information.

It is therefore fitting that California's leadership in the development of sophisticated information technologies is matched by its attention at this time to the development of a set of privacy principles to guide government agencies and private sector entities alike in the handling of personal information.

It is fitting that privacy principles are being discussed at this time for another reason. The European Union's (EU) Data Protection Directive will be enacted in October 1998. The Directive states that the transmission of personally identifiable information from one of the member countries to any country without "adequate" privacy protection will be prohibited. (Chapter IV, Article 25: "Member States shall provide that the transfer to a third country of personal data ... may take place only if ... the third country in question ensures an adequate level of protection.")

The United States lacks an omnibus privacy protection law. We have instead taken the sectoral approach, adopting specific laws for industries such as credit reporting, cable television, and video records. Policy analysts predict that the data of, say, multinational corporations based in EU countries will be restricted from transmitting personally identifiable data into the U.S. because we have no over-arching privacy law. Nor do we have a Privacy Commission as do the European nations, Canada, New Zealand and Australia. By adopting privacy principles, perhaps California can be the first state in the nation which passes the "adequacy" test of the European Union vis-a-vis its Data Protection Directive.

Source of principles: The following nine principles have been adapted from several existing sets of "fair information practices," developed since the early 1970s. Key among these are the U.S. Department of Health, Education and Welfare Fair Information Practices (1973), the international principles of the Organization of Economic Cooperation and Development (OECD, 1980), and the Canadian Standards Institute Privacy Code (1996).

Format of principles: For each of the nine principles, the following issues are discussed: (1) why it is needed; (2) the issue(s)/scenarios addressed by the principle, including situations where the principle was not applied and harm occurred; and (3) precedents, where the principle has been applied in law and/or industry practice.

Definition: The word "organization" is used broadly to also mean government agency, business, nonprofit, association, etc.

* *

1. Principle of proactivity. *Privacy implications are recognized explicitly and shall be considered when personally identifiable information is to be collected, accessed, stored, merged or otherwise manipulated, and when the application of any new information technology is introduced.*

Why it's needed: It is important that privacy implications be considered proactively rather than reactively. Actions taken by state or local government in which personally identifiable information is at issue can have significant impacts on individuals' privacy. This includes legislative action, regulatory agency decisions, court decisions, and government-funded programs administered by private businesses under contract with a government agency.

Likewise, the personally identifiable information collected and disseminated by private sector entities can also impact individuals' lives. Information compiled in a variety of commercial data bases is used to make decisions about employment, insurance, health care, and credit, to name just a few applications.

The privacy implications of new technologies and new applications of existing technologies must be considered before the information infrastructure is developed. Ignoring privacy implications up front leads to retrofitting the system after the fact -- an expensive proposition, not only in economic terms, but also societal and personal. Once privacy has been lost, it is difficult, and often impossible, to restore.

Issue(s)/scenarios addressed: In the past five years, there have been numerous examples of what happens when information technologies are introduced without first considering the privacy implications.

- In 1996, Lexis-Nexis launched its P-Trak "people finding" service, which included the sale of individuals' Social Security numbers. The resulting public outcry prompted Lexis-Nexis to alter the product to exclude the SSN.

- In February 1998, the *Washington Post* reported that two large supermarket chains with in-store pharmacies, Giant and CVS, were selling customers' prescription information to a Massachusetts company. That company, Elensys, in turn arranged with drug manufacturers to pay the pharmacies to have "educational" messages and solicitations mailed to the customers with particular ailments. Within two days of the news story, both Giant and CVS announced they were curtailing the practice due to the negative response from their customers.

- In March 1997, the U.S. Social Security Administration began offering access to individuals' Personal Earnings and Benefit Estimate Statement (PEBES) on its Internet web site, www.ssa.gov. Due to immediate public criticism regarding insufficient safeguards to prohibit access by unauthorized users, the SSA suspended operation just one month later. It then launched a series of public forums in which it invited input from private sector high-tech businesses, consumer advocates and public officials. Its resulting implementation plan can be considered a model for any entity which introduces applications of information technologies involving personally identifiable information. The SSA implementation plan includes

  (1) the development of a privacy and security policy for online services,

  (2) ad hoc advisory assistance from experts,

  (3) the preparation of privacy impact assessments on significant projects, and

  (4) publication of a periodic privacy review for public dissemination.

[*Privacy and Customer Service in the Electronic Age: Report to Our Customers* , U.S. Social Security Administration, Publication Number 03-012, Sept. 1997, p. 32.]

The growing practice of government agency "data matching" deserves some special consideration here regarding the principle of proactivity. On both the state and local government levels, government agencies in California are engaged in initiatives which involve the merger of data across several agencies. In San Diego County, for example, the Department of Health and Human Services, is developing a "Consolidated Client Index." Another such endeavor is Project Heartbeat which would merge the various data bases of agencies that serve at-risk youth. The latter is the subject of Assembly Bill 1801 (Davis) which would enable the agencies to share data with one another via a pilot project in San Diego County.

At the state level, the California Department of Education has been studying ways to develop standards for the handling of K-12 student records to enable records to be more efficiently merged and transferred when a student moves to another school. This program is conducted in conjunction with the development of a nationwide standard called SPEEDE/ExPRESS, with the ultimate purpose of being able to develop a longitudinal data base of public school student records wherever they might have attended school.

The merger of government agency records, while desirable from the standpoint of cost savings and efficiency of services, is often viewed as the ultimate in "Big Brother" endeavors -- a cradle to grave dossier on each of us. If the principle of proactivity is to be applied anywhere, it should certainly be applied in any data matching programs proposed by government agencies. By conducting a privacy impact assessment, government will be able to determine the consequences, both intended and unintended, of such programs. And by applying the remainder of the privacy principles as discussed below, policy makers will be able to further evaluate whether or not the particular data matching program is sound public policy vis-a-vis personal privacy considerations.

Precedent: There are many situations where the principle of proactivity is required and practiced. When legislation is crafted, the fiscal implications must be charted. In the construction of highways and other major building projects, the environmental impact must be assessed. The City of San Diego adopted a privacy policy in October 1996 (900-13) which includes "consideration of privacy effects" as a principle when "introducing and using information technologies."

The implementation of Caller ID in California serves as an excellent example of the principle of proactivity at work. When the local telephone companies proposed to implement Caller ID in the early 1990s, the California Public Utilities Commission (CPUC) held several public forums around the state. It learned that privacy was a significant concern of those who participated. About half of those who testified and submitted written comments thought Caller ID would severely invade their privacy. The other half thought it would enhance their privacy.

The CPUC's resulting decision in 1992 (92-06-065) required that the local telephone providers (Pacific Bell, GTE and several regional companies) educate consumers about the privacy implications of the service before Caller ID could be implemented. Indeed, when the service was introduced in 1996, an extensive consumer education campaign was launched to raise Californians' awareness of the privacy implications of the service and to inform them of their number blocking options.

2. Principle of secondary use. *Personal information shall not be used or disclosed for purposes other than those for which it was collected. Secondary usage of information is permitted only with the affirmative consent of the individual.*

Why it's needed: The restriction on secondary uses of information is at the heart of all privacy policies dating back to the original code of Fair Information Practices, adopted by the U.S. Department of Health, Education and Welfare in 1973. There is a tremendous temptation, especially in this age of powerful computers and decreasing costs of operation, to find additional uses of information. Author Erik Larson, in *The Naked Consumer* , discusses the universal laws governing the flow of data collected about individuals. One such law is that "data *always* will be used for purposes other than originally intended. (Henry Holt and Co., 1992, p. 14)

The individual who enters into a transaction with a service provider such as a merchant fully expects the information that is divulged in that transaction to be used solely to complete the transaction, and perhaps to do business with that entity in the future. Such transactional data might include a credit card number, name and address, a Social Security number, a driver' license number, sizes of clothing, brand names and quantity of supermarket goods, tastes in music, titles of books, videos rented, and so on.

Such data has considerable value beyond the initial transaction. And therein lies the temptation of secondary use -- the use of that information for purposes other than the original reason for gathering it.

Given the increasing digitization of our various daily transactions, the possibility exists that the totality of information collected will be merged to form a comprehensive picture of each of us, an "electronic dossier." The secondary uses of this comprehensive data set are virtually limitless, with the most troubling of them involving surveillance and social control.

As with many of these privacy principles, the principle of secondary usage works in conjunction with other principles, especially relevance and affirmative consent, discussed below. Because information often has value for secondary uses, the information gatherer is likely to want to collect additional information to enhance the value. The principle of relevance (number five) states that only the information necessary for the matter at hand shall be collected. And if information is to be sold, exchanged or otherwise made available for secondary uses, permission from the individual must be obtained -- the principle of affirmative consent (number four).

Issue(s)/scenarios addressed: There are many examples in which personally identifiable information, collected for one purpose, is put to secondary uses without the consent of the individual.

- Perhaps the most prevalent example of a violation of the principle of secondary usage concerns Social Security numbers. The SSN was originally developed as a record-keeping number for the Social Security Administration's management of U.S. citizens' retirement benefits. Some restrictions were placed on secondary uses of the SSN by the federal Privacy Act of 1974, but only by local, state and federal government agencies. These restrictions have been watered down over the years.

- But no restrictions have been placed on private sector entities, resulting in significant

secondary use of the SSN and tremendous harm to individuals. Insurance companies use the SSN as subscriber ID numbers. Cable companies use it to identify their customers. Employers use it as the employee ID. Colleges and universities use the SSN as the student number. The financial industry (credit, banking) uses the SSN as customer identifiers, and even as PIN numbers.

- It is the financial industry's use of SSNs that has contributed to the crime of identity theft, estimated to victimize a half a million Americans a year. Imposters who obtain someone's SSN -- a relatively easy matter given the SSN's profligate use throughout society -- can apply for credit in the victim's name and open bank accounts. They rack up thousands of dollars of expenses in the victim's name before reaching the credit limits on each account, and then move on to someone else's identity. Victims are left with a ruined credit history, and must spend months and even years regaining their financial health. Identity theft results in billions of dollars in fraud annually, not to mention the loss in productivity to the victims who must spend many hours and days cleaning up their credit.

- Had the SSN been prohibited from being used as an identifier by private sector entities, and had it not been adopted as the key to consumers' finances, we are likely not to be experiencing the explosion of identity theft crimes today.

- Another example of secondary use is the credit "header," which has taken on a life of its own as a "people-finding" tool. Yet, its original purpose was simply to provide the necessary identification for credit grantors using the individual's credit report to make a decision regarding the extension of credit.

- The so-called "product registration" form is another example of violation of the secondary use principle. While the ostensible use of this form is to identify the person who has just purchased a product which has a warranty, the information collected on the form -- hobbies, income, education, home ownership -- is used by marketers to solicit other goods and services to that individual. It should be noted that this form usually includes a disclosure and consent statement at the end. But it is written in such small type and vague language that it is questionable whether the statement truly meets the standard of informed consent as required in this principle.

Precedent: There are many precedents in law regarding secondary usage.

- The Privacy Act of 1974 (5 USC 552a), which applies to federal government agencies, states that information collected for one purpose shall not be used for other purposes without first getting the permission from the individual.

- California's own version of the Privacy Act, the Information Practices Act (Civil Code 1798) states in its "legislative declaration and findings" that "in order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits."

- Recently, the Federal Communications Commission issued a ruling which restricts secondary use of telephone records. Telecommunications companies must obtain customer consent before they can use their records, calling patterns and other personal information to market new services to them.

- California voter registration records have been restricted to political-related and research uses.

- California Department of Motor Vehicles records have been restricted to specific uses since the actress Rebecca Schaeffer was murdered in 1989 by a stalker who obtained her residential address.

3. Principle of access. *An organization shall make specific information available to individuals about its policies and practices relating to the handling of personal information. Individuals shall have reasonable means to learn about, obtain and review, and when necessary, correct and amend information about themselves.*

Why it's needed: Information in a wide variety of data bases is used to make critical decisions about each and every one of us. For example, when an individual is turned down for a job, an apartment, or a loan, he or she must be able to determine whether or not the information used to make that decision was accurate. Access to that information is necessary to make this assessment.

Access is also at the foundation of laws regarding government compilation of personally identifiable information. It is especially critical in a democratic society that citizens have a right of access to information about them in order to prevent abuse of power.

An often overlooked aspect of access is education about how access can be obtained. Reasonable efforts must be made to educate individuals about the existence and use of personally identifiable information held by the organization. Education efforts should include how personal information is obtained, used, stored and disclosed, as well as individuals' rights as expressed in these privacy principles.

It should be noted that California has a long tradition of encouraging and requiring consumer education to lessen the harmful impacts of the introduction of information technologies (for example the California Public Utilities Commission's Telecommunications Education Trust). When consumers are informed, they are better able to make decisions to safeguard their personal information.

Issue(s)/scenarios addressed: While access is a major part of several privacy-related laws, there are still significant gaps where consumers lack access.

- The compilers of consumer profile information in the direct marketing industry do not afford consumers access to records about them. Companies such as Metromail, Polk, and Database America, to name a few, have not developed the necessary infrastructure to enable consumers to learn what their records contain.

- The California Information Practices Act, which gives citizens the right to obtain the records compiled about them by state government agencies, has been weakened significantly since the Office of Information Practices was defunded and closed in the early 1990s. That office was instrumental in monitoring access procedures and informing citizens of their right of access. Without this office, the state has no idea of the totality of data bases containing personally identifiable information compiled by state government agencies. And individuals have no

"one-stop shopping" clearinghouse for information about their access rights.

Precedent: There are a number of laws addressing access to both private and public sector data bases.

- Access is at the heart of both the federal Freedom of Information Act and the Privacy Act of 1974. California's equivalents to those acts also include strong rights of access: the Public Records Act and the Information Practices Act.
- The federal Fair Credit Reporting Act and its California equivalent give consumers a right to obtain their credit report and correct errors. That right also includes being told who else has accessed that report.
- The federal Cable Communications Policy Act gives subscribers the right to inspect and correct errors in their account record. California also has its version of this law.
- Several other California laws provide individuals with access to their personal records held by private sector entities. Californians have a right of access to their medical records, something not available in about half the states. We also have a right of access to our employment records. And the Insurance Information and Privacy Protection Act provides access to insurance records.

4. Principle of affirmative consent. *The knowledge and consent of the individual are required for the collection, use or disclosure of personal information.*

Why it's needed: The definition of informational privacy revolves around control -- the right of individuals to determine when, how and to what extent they will divulge personal information about themselves to others. [Adapted from Alan Westin, *Privacy and Freedom* , Athaneum, 1967] The foundation of the principle of affirmative consent is the ability of the individual to control his or her personal information.

With the proliferation of data bases containing ever increasing amounts of information about us, the principle of affirmative consent becomes even more important. The totality of information in data bases is being referred to by some as our "digital persona," an entity that is taking on a life of its own. Certainly, when we are represented in a multitude of transactions by a virtual being that is comprised of many discrete bits of data about us, we must be able to control the development of our digital persona through the principle of affirmative consent.

This principle is also at the foundation of a democratic society, both in our relationship to government entities, as well our transactions with the private sector. With affirmative consent fully in force, secret information collecting is restricted.

Issue(s)/scenarios addressed: The word "affirmative" has been added to "consent" in this principle for a specific reason. Often, consent is obtained invisibly. It's a "negative option" hidden in wording in the fine print, for example the Conditions of Use language that individuals receive when they become a customer of a bank or credit card company. Few people read or understand such language. And as a result, they give consent for their data to be disclosed to third parties without realizing it.

Another way consent is obtained is through coercion. The Privacy Rights Clearinghouse has learned of numerous companies which refuse to provide service to individuals who will not disclose their Social Security number, for example, some cable TV companies, some medical clinics, some insurance providers, and virtually all cellular phone companies. The PRC has also received complaints from individuals who have been fingerprinted at banks as a requirement to cash noncustomer checks. If they do not consent to being fingerprinted, they are not able to cash the check.

Electronic communications afford many ways for personal data to be compiled without the individual knowing it. Here are some examples:

- A few years ago, a pharmaceutical company advertised an 800 number which allergy sufferers could call to obtain the pollen count in their city that day. Unbeknownst to them, their phone numbers were collected by the drug company through a process called Automatic Number Identification (there is no way to block the transmission of phone numbers when calling 800 and 900 numbers, even when the Caller ID blocking code *67 is used). Using a reverse directory, the drug company obtained the names and addresses of those callers and sent them mail solicitations about its new allergy medication.

- Electronic mail addresses are "harvested" by software programs and then used by marketers to send "junk" e-mail solicitations, also called "spam," to millions of Internet users. Such solicitations are sent without consent. They clog the information superhighway and are the source of numerous complaints to Internet providers and lawmakers. Bills currently before the California Legislature and Congress would require consent.

- When individuals "surf" the Internet, their "clickstream" can be compiled invisibly. These electronic footprints can then be merged into a detailed profile of the individual's interests. Many web sites require that users register before proceeding further, revealing their names, addresses and other personal information. Few such web sites provide privacy policy statements which disclose what is done with such information and whether or not there is the option to restrict third party use of the data. A recent survey conducted by the Federal Trade Commission found that only a small percentage of sites disclose their information collection activities. In a majority of sites, disclosure and consent are absent.

The debate of "opt-in" vs. "opt-out" is at the heart of the affirmative consent principle. When opt-out is practiced, the entity that gathers and disseminates the information assumes consent unless the individual indicates that the information is not to be used, a kind of "negative option." The personal information is disseminated until the time that the individual exercises the opt-out option, if at all.

When opt-in is practiced, it is assumed that the individual does <u>not</u> consent to information being collected and used. Affirmative consent must be provided before the individual's personal information is used. Opt-out is the norm in this country. If the principle of affirmative consent were truly practiced, opt-in would guide the collection and dissemination of personal information.

Generally, the opt-in option is used in situations where sensitive personal information is compiled and used, such as medical records. But California's medical records confidentiality law contains a troubling example of opt-out. The opt-out clause is italicized.

> California Civil Code 56.16. "*Unless there is a specific written request by the patient to the contrary* , nothing in this part shall be construed to prevent a provider, upon an inquiry concerning a specific patient, from releasing at its discretion any of the following information: the patient's name, address, age, and sex; a general description of the reason for treatment ...; the general nature of the [treatment], the general condition of the patient; and any information that is not medical information as defined in subdivision (c) of Section 56.05."

How many patients will think to carry a written document to the hospital which instructs staff not to disclose information about their treatment there? That is the nature of opt-out, and the reason the word "affirmative" is added to the principle of consent. In an opt-out scenario, the burden is on the consumer to prohibit the release of information about them. Few consumers are sufficiently aware and proactive to take such action. The practice of opt-in places the burden on the information user to obtain consent from the individual. This enables the individual to be fully informed of the uses to be made of the information and to have the opportunity to exercise the option without coercion.

We close the discussion of affirmative consent by looking at an emerging technology that will test the very efficacy of this and the other principles. Advancements in the technology of video surveillance present several challenges to the principle of affirmative consent. Satellites are now capable of recording images on the ground to the resolution of a few square feet. (Government satellites engaged in intelligence gathering can record images to the resolution of a few inches, although these are not available for commercial use.) Back on earth, video surveillance cameras are becoming commonplace in business establishments, public places, schools, and the workplace. Digital video technology already exists, although not yet for broad commercial use, that can scan faces and obtain "face prints," similar to fingerprints in that they comprise a unique individual identifier. With such technology, a crowd could be scanned, and the identities of those present can be known, certainly a chilling possibility, one rife with implications for our civil liberties.

The privacy implications of video and satellite technology are just now emerging. These sophisticated technologies bring into question the principle of affirmative consent, as well as the other principles. They present a challenge for policy makers attempting to limit the many privacy intrusions facing citizens in this information age.

Precedent: A recent amendment to the federal Fair Credit Reporting Act provides individuals with an important right of affirmative consent. When an employer conducts a background check on a job applicant, it must obtain the affirmative consent of that person. (And if a negative hiring decision is made, the applicant must be able to obtain a copy of the report, an example of the access principle, discussed above.)

California law requires consent of <u>all</u> parties before a telephone conversation can be recorded. We are one of only 12 states with an all-party recording law.

Another example of consent is the medical records release form signed by patients to enable their health care provider to release information about the patient to other health care providers and to the insurance company, required under California's medical records confidentiality law, Civil Code 56. Unfortunately, many such release forms are worded broadly. And the element of coercion can be present in such transactions -- no signature, no service.

5. Principle of relevance. *The collection of personal information shall be limited to that which is necessary for the transaction with the individual and purposes identified by the organization. The purpose for which personal information is collected should be specified at the time of collection. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.*

Why it's needed: The advancement of computer and telecommunications technologies enables companies to collect tremendous amounts of personal information, merge it with other data, and analyze it to find previously unknown relationships. Witness the growth of "data mining" and "data warehousing" in the service and financial industries for the purpose of "database marketing." This growing practice enables the company to learn as much as possible about its customers in order to target products and services to them. Government agencies are also examining the practice of data warehousing, merging the contents of numerous data bases of many agencies into one record, to be used for a variety of applications.

With these vast data collection capabilities come the temptation to use the data for other purposes, and to take advantage of the data's commercial value by selling it to third parties. It should be noted here the particular danger that arises from the commercial use of government information. In order to increase the monetary value of their data, cash-strapped government agencies might collect more information than is needed for the matter at hand. Indeed, government agencies are already selling public records information to private sector information vendors, who in turn package the information and sell it to any number of users. Without strict adherence to the principle of relevance, government agencies may be encouraged to increase the revenue potential of their data by collecting more than is needed.

The principle of relevance places restrictions on the amount of time information can be retained and disseminated. This brings the notion of "social forgiveness" into the discussion. Should, for example, someone's graffiti vandalism conviction at age 19 prevent that person from getting a job 10 years later when his life has been turned around and earlier misdeeds are no longer relevant?

The principle of relevance also limits the element of coercion in the provision of services. In both the private and public realms, individuals are often required to divulge specific information to obtain a good or service -- for example, name and address for telephone service. The principle of relevance prohibits the collection of extra information, unrelated to that good or service.

The principle of relevance works in conjunction with other principles, notably secondary usage. Issues surrounding this principle have been discussed in number two above and are summarized here:

- These two principles collectively prevent the over collection of information.
- They inhibit the development of extensive dossiers on individuals.
- They require the organization or agency to specify the purpose for which it is collecting the data at the time of collection.

Issue(s)/scenarios addressed: Significant related discussion has already been presented under the principle of secondary usage above. We focus the discussion here on the ultimate question regarding relevance, whether there are situations in which it is appropriate to gather no personally identifiable

information -- the issue of anonymity.

We are swiftly approaching the time when virtually all of our daily transactions are conducted via systems in which data is collected. Technology forecasters describe the day when we will all carry multi-purpose "smart cards." These will take the place of cash, driver's licenses, credit and debit cards, library cards, employee ID cards, highway toll-booth recording systems, student IDs, phone cards, health insurance cards, and so on. Smart cards might also hold our medical records, our vital documents such as birth and marriage certificates, and our voter registration form, to name a few applications.

We can all no doubt understand the significant convenience of smart cards. But the privacy-related threats are evident as well. The totality of "electronic bread crumbs" that we leave along our life-long path comprises a comprehensive dossier of who we are. The potential uses of such robust data dossiers give rise to chilling scenarios of surveillance and social control.

The ultimate test for anyone applying the principle of relevance is to ask the question: Is any personally identifiable data required for the application under consideration? Does the cash component of a smart card require the disclosure of one's identity when used at the supermarket, the newspaper vending machine, the subway, the soda machine, the phone booth, or the parking meter? Does the automated highway toll collection booth need to know that Jane Smith passed the recording station at such and such a time? Or is it sufficient to note that account number 54321 was just debited for the amount of the toll. Should data be collected only because it can be gathered, given the power, ease and affordability of computer technology? Or shall we build anonymity into information technologies when appropriate? That will be the true test of the principle of relevance.

Precedent: There are several federal and state laws which embody the principle of relevance, or collection limitation.

- The federal Privacy Act, for example, requires the agency to determine that the information it has on file is relevant to the mission of the agency. California's version of the Privacy Act, the Information Practices Act, requires that the purpose for which the information is gathered be specified in a notice provided to the individual when the information is collected. But the IPA does not appear to contain a collection limitation clause per se. It should be noted that the IPA only pertains to state government records, not to personally identifiable information at the local government level.

- California law places limits on the information collected by merchants when customers pay for goods or services by credit card. California Civil Code 1747.8 prohibits the collection of information other than that provided on the credit card -- name, account number and expiration date -- with specific exemptions for situations where, for example, a product must be delivered to a residence. The credit card transaction can be successfully completed with the limited information provided on the card. This law prevents the collection of additional information in order to deter fraud and to protect the privacy of the card holder. It restricts the collection of address and phone number information that might enable the merchant to compile a data base of customers for solicitation purposes.

- Another example of the principle of relevance can be found in labor law. Employment laws at the federal and state levels prohibit certain questions to be asked of job applicants in order to prevent discrimination based on age, sex, marital status, race and other factors.

The principle of relevance also contains a clause regarding retention of records. Both federal and state credit reporting laws place limits on the length of time negative information can be indicated on one's credit report. Debts more than seven years old must be removed; and bankruptcy information must be removed after ten years. Another example of records retention limitations involves driving records. The California Motor Vehicles code places limits on the length of time certain driving violations can be part of one's record.

6. Principle of accuracy. *Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.*

Why it's needed: Many important decisions are based on information held in data bases -- whether one get a job, can rent an apartment, receives insurance, is extended an automobile loan or a mortgage, or is granted a credit card, to name a few situations. For decisions to be made fairly, information must be accurate and up to date.

This principle functions in conjunction with the principle of access. The individual must be able to obtain and review his or her record in order to know whether or not it is accurate.

Issue(s)/scenarios addressed: The annals of the Privacy Rights Clearinghouse are replete with stories of individuals who have been harmed by erroneous information -- a credit report which contains an imposter's credit history, for example; a record in the Medical Information Bureau data base which has been miscoded, indicating a serious medical condition when there is none; a criminal record pulled for the wrong John Smith, resulting in employment denials; to name a few.

The Bronti Kelly case has recently received attention in the news. It provides a classic example of the harm that can befall individuals when data bases contain erroneous information. The Kelly case also exemplifies the importance of adhering to the principle of access (number three).

> In the early 1990s, Bronti Kelly was employed by a major department store for a time, and was laid off. He then attempted to obtain employment at many other department stores in Southern California to no avail. With no income, he became homeless. Kelly finally landed a job at a department store, but after one week was laid off. In frustration, he pressed the human resources manager for the reason he was fired. He was told that a few days after he started work, the company accessed an employment background check service which listed Kelly as having been convicted for shoplifting. Kelly then realized that an imposter who had stolen his wallet years before had been carrying his identification documents when committing crimes, thereby giving Kelly a criminal record.
>
> During his long period of unemployment, Kelly had not been notified about the data base that had been used to make negative employment decisions about him. He therefore had no opportunity to alert employers to his erroneous criminal record. The privacy principles of both accuracy and of access had not been followed by the companies to which he had applied for work. Kelly sued both the department store company and the background check service. He won a small judgment against them in January 1998.

It should be noted that as of October 1997, amendments to the federal Fair Credit Reporting Act requiring disclosure and consent in the background check process would prevent the Bronti Kelly case from happening today.

Precedent: There are strong precedents in both federal and state laws regarding the accuracy of personally identifiable information. The federal Privacy Act and California's Information Practices Act contain provisions which enable individuals to correct or amend erroneous information in government agency records.

In the private sector, the Fair Credit Reporting Act and its California equivalent contain provisions for the correction of erroneous information, and sanctions if records are not corrected. The federal Fair Credit Billing Act contains a similar provision. Additional federal laws in which the individual is able to challenge the accuracy of records and have them corrected include the Family Educational Rights and Privacy Act (FERPA) and the Cable Communications Policy Act. There are similar laws at the state level.

Additional laws at the state level which give individuals the right to have records corrected or amended are the Insurance Information and Privacy Protection Act, and the Medical Records Confidentiality Act.

7. Principle of security. *Reasonable physical, technical and administrative safeguards will be taken to protect personal information against the risk of unauthorized access, collection, use, disclosure or disposal.*

Why it's needed: The thought of computer hackers often comes to mind when information security is considered. Likewise, the necessity for encryption of data is often seen as the cure-all for information security. Indeed, the use of privacy-enhancing technologies like encryption is essential in order to safeguard data, especially personally identifiable information that is particularly sensitive. But such high-tech applications are not the total solution.

Security goes much further than protecting computer systems from outside intruders. There is also the threat of "insiders" who take advantage of their access to personal information to browse records without proper authorization, and perhaps to provide information to illegitimate users for a price. There are also those within the organization who are unwittingly "conned" into disclosing information.

An all-too common security breach is disposing of records without shredding them. Investigators of identity theft cases often report that the imposter was able to obtain the information needed to commit the crime by retrieving unshredded credit card transaction slips and loan applications from dumpsters. Indeed, many of the privacy abuses reported to the Privacy Rights Clearinghouse are the result of "low-tech" security breaches.

Information has value to a multitude of users who are not authorized to have access to it. The principle of security is therefore central to any code of privacy protection.

Issue(s)/scenarios addressed: We are reminded daily of the implications of inadequate security of

personally identifiable information. Here are a few examples which illustrate both low-tech and high-tech security breaches.

- A student requested a copy of her file from the Student Aid Commission. When it arrived, she was shocked to find that in addition to her file, the names, addresses, Social Security numbers and phone numbers of 20 other people were in the same envelope. They had been included by accident by a Commission employee.

- Before departing the singles dating service office, a fired employee stole a computer diskette containing the supposedly confidential mailing list of all its clients. He sold the list to other dating services in the area.

And these stories of medical records security breaches from news reports:

- An employee of an AIDS assistance center downloaded the names of 4,000 HIV-positive patients and mailed the computer diskettes to two Florida newspapers.

- A psychiatric hospital employee anonymously faxed the medical records of a member of Congress to the *New York Post* on the eve of her Congressional primary election. She awoke to a front-page story of her attempted suicide. She won the race, despite the story.

A crime that perhaps best symbolizes the nationwide absence of a "culture of confidentiality" is identity theft. This fast-growing crime is largely a result of societywide security lapses:

- Many credit grantors do not check the identity of applicants adequately Credit bureaus are allowed to sell credit "headers," which include the Social Security number, without restriction. Many businesses do not shred documents before putting them in the dumpster. Organizations of all types allow employee access to sensitive information, including employees' and customers' Social Security numbers, without password protection or need-to-know authorization. Even the federal government has been instrumental in this crime by allowing the SSN to be used as health insurance account numbers and as student ID numbers in countless schools, colleges and universities. The SSN is thereby carried on plastic cards in tens of millions of wallets.

Precedent: There are several laws in which security is mandated. But such laws are generally limited in effectiveness because of loopholes and weak sanctions. Clearly, for the security principle to be effective, it must be grounded in policies and procedures with significant sanctions.

The federal Fair Credit Reporting Act and its state equivalent contain clauses which prohibit individuals' credit histories from being obtained by anyone without a "legitimate business purpose." There are penalties, albeit limited, for illegitimate access.

California's Medical Records Confidentiality Act restricts who can access individuals' health care information, although with some loopholes, and with limited sanctions for improper disclosure.

Outside the realm of laws, security-minded organizations, including government agencies, corporations and nonprofit organizations, have adopted privacy policies which include the requirement that employees who handle personal information sign confidentiality agreements. This practice is expected to grow as organizations realize the high costs of lawsuits, lost productivity and

low morale that accompany inadequate security.

8. Principle of accountability. *An organization is responsible for personal information under its control and shall designate a person who is accountable for the organization's compliance with the principles. An individual shall be able to challenge compliance with the above principles with the person who is accountable within the organization. A mechanism for oversight and enforcement shall be established to ensure the observance of these principles.*

Why it's needed: A common complaint of consumers is their inability to find someone within the organization, whether it's a government agency or a company, who is responsible for the handling of personally identifiable information and who can take action when privacy abuses have occurred. They are further frustrated at not being able to gain redress for the invasion of their privacy. Clearly, there exists an "accountability void" in public and private sectors alike.

Issue(s)/scenarios addressed: Included in Precedent, below.

Precedent: It is difficult to find strong precedents for information accountability in the operation of government agencies and in corporate practices. This is perhaps a result of the absence of an omnibus privacy protection law in this country.

The accountability principle is crucial to the successful implementation of the totality of the privacy principles. But there are few role models on which to apply this principle. A significant challenge facing those who adopt the privacy principles is crafting an effective mechanism for accountability.

Both the federal Privacy Act and the California Information Practices Act are weak vis-a-vis the principle of accountability. Neither law clearly requires an agency to develop an infrastructure for accountability. The Information Practices Act was significantly weakened in this regard in the early 1990s when the Office of Information Practices was defunded by the Legislature. An additional weakness of the IPA is that it only pertains to state government agencies, and does not extend to the local level where there are significant compilations of personally identifiable information. On the federal level, the U.S. Office Management and Budget oversees the Privacy Act, but is virtually invisible in this function.

Clear accountability mechanisms for information handling in the private sector are also difficult to find. Consumers who have complaints about how their own information was handled often experience being referred from department to department. Many give up the exercise of gaining redress for their grievance when they realize their only recourse is to sue the company. But that's hardly an option for most individuals who are no match for the corporation's "deep pockets" and extensive legal resources.

Perhaps the answer to the "accountability void" lies in nontraditional strategies. Alternative dispute resolution, for example, might well prove to be highly effective in resolving many of the disputes consumers have with companies and government agencies alike. Indeed, the Privacy Commissioners in New Zealand and in the province of Quebec, where there are omnibus privacy laws covering both the private and public sectors, report that the majority of all privacy disputes which they handle are resolved through mediation.

Public disclosure of privacy abuses might also prove effective -- perhaps a web sites which individuals can access to find out whether company X or government agency Y engages in practices contrary to these privacy principles or even its own privacy code.

Such nontraditional mechanisms as alternative dispute resolution and an online complaints web site would likely need some type of oversight body. In this decidedly non-regulatory era, this too calls for creative thinking. Is there a place for a "privacy monitor," either within state government or established in the nonprofit sector? Can an entity be created which provides incentives for responsible information practices, such that sanctions for bad practices are required in only the most grievous instances where mediation and public disclosure have failed? Such an entity might have the following functions:

- Promote alternative dispute resolution.
- Shine the spotlight on good privacy practices as well as bad, whether in the public, private or nonprofit sectors.
- Foster extensive consumer education to make individuals more privacy vigilant.
- Encourage adoption of privacy principles and serve as a stamp of approval.
- Conduct research and publish reports on policy alternatives, uses of technology, and other issues. Convene public forums to discuss controversial issues.

9. Principle of progress. *As information technologies advance, privacy considerations are likely to change. The principles will be reviewed on a regular basis to ensure their adequacy.*

Why it's needed: Information technologies are advancing at breakneck speed, spawning applications that are ever-changing. By the same token, the privacy implications of information-based services are also changing. The principles adopted today may not be effective for the technology of tomorrow. Therefore, periodic review of the principles is necessary to ensure their relevance and efficacy.

Issue(s)/scenarios addressed: The need for ongoing review and revision of the privacy principles can be illustrated by the evolution of Caller ID in California. Caller ID was implemented by local telephone companies in 1996, after many years of wrangling over the issue. The service allows the subscriber to view the telephone number of the calling party on a display device next to the phone.

The California Public Utilities Commission required that extensive public education about the privacy implications of this service be conducted by the phone companies and by numerous community-based organizations which were awarded grants. The education campaign focused on the use of blocking mechanisms, available free to consumers. As a result of the education campaign, over half of households chose the strongest form of privacy protection, Complete Blocking.

But Caller ID is not a static service. Now, the phone companies want to add the person's name to the telephone number, so that when the called person looks at the display device next to the phone, both the number and the name of the caller will be shown. This represents a significant enhancement, or

privacy intrusion, depending on your point of view. Whether the CPUC addresses this addition to Caller ID with the attention it initially focused on the fledgling service remains to be seen. It is not likely, however, that the same level of care will be taken to educate Californians about the privacy implications of "advanced Caller ID."

Precedent: The principle of review is well-established in public policy proceedings. For example, "sunset review" is a mechanism the Legislature uses to comprehensively review the need for and performance of administrative agencies that it has created.

If privacy principles are adopted through legislation or through informal agreements, a recurring requirement should be established to review the principles vis-a-vis enhanced information technologies and other developments that we cannot foresee at this time. If the principles are established through legislative action, the review process could perhaps be delegated to an entity like the Little Hoover Commission or the Bureau of State Audits.

Privacy Rights Clearinghouse

More About Us | Fact Sheets | Other PRC Resources
Privacy Links | Cases | About Our Book | Identity Theft Resources | E-mail

HOME

Attachment D

Edit Document

Enter Category:
ITS Fair Information and Privacy Principles

Enter Title:
Draft Final - Intelligent Transportation Systems Fair Information and Privacy Principles

Enter the page below:

Draft Final
Intelligent Transportation Systems
Fair Information and Privacy Principles

These fair information and privacy principles were prepared in recognition of the importance of protecting individual privacy in implementing Intelligent Transportation Systems. They have been adopted by ITS America in draft final form. The Privacy Task Group of the Legal Issues Committee will present these principles for review and comment to organizations and groups interested in privacy and ITS outside of ITS America during 1995. They will then be submitted for final adoption to the ITS America Legal Issues Committee, Coordinating Council, and Board of Directors.

The principles represent values and are designed to be flexible and durable to accommodate a broad scope of technological, social, and cultural change. ITS America may, however, need to revisit them periodically to assure their applicability and effectiveness.

These principles are advisory, intended to educate and guide transportation professionals, policy makers, and the public as they develop fair information and privacy guidelines for specific intelligent transportation projects. Initiators of ITS projects are urged to publish the fair information privacy principles that they intend to follow. Parties to ITS projects are urged to include enforcible provisions for safeguarding privacy in their contracts and agreements.

1. *INDIVIDUAL CENTERED.* Intelligent Transportation Systems (ITS) must recognize and respect the individuals interests in privacy and information use.
ITS systems create value for both individuals and society as a whole. Central to the ITS vision is the creation of ITS systems that will fulfill our national goals. The primary focus of information use is to improve travelers' safety and security, reduce travel times, enhance individuals ability to deal with highway disruptions and improve air quality. Traveler information is collected from many sources, some from the infrastructure and some from vehicles, while other information may come from the transactions like electronic toll collection that involve interaction between the infrastructure and vehicle. That information may have value in both ITS and non-ITS applications. The individuals expectation of privacy must be respected. This requires disclosure and the opportunity for individuals to express choice.

2. *VISIBLE.* Intelligent transportation information systems will be built in a manner visible to individuals.
ITS may create data on individuals. Individuals should have a means of discovering how the data flows operate. Visible means to disclose to the public the type of data collected, how it is collected, what its uses are, and how it will be distributed. The concept of visibility is one of central concern to

the public, and consequently this principle requires assigning responsibility for disclosure.

3. *COMPLY.* Intelligent Transportation Systems will comply with state and federal laws governing privacy and information use.

4. *SECURE.* Intelligent Transportation Systems will be secure.
ITS data bases may contain information on where travelers go, the routes they use, and when they travel, and therefore must be secure. All ITS information systems will make use of data security technology and audit procedures appropriate to the sensitivity of the information.

5. *LAW ENFORCEMENT.* Intelligent Transportation Systems will have an appropriate role in enhancing travelers' safety and security interests, but absent consent, government authority, or appropriate legal process, information identifying individuals will not be disclosed to law enforcement.
ITS has the potential to make it possible for traffic management agencies to know where individuals travel, what routes they take, and travel duration. Therefore, ITS can increase the efficiency of traffic law enforcement by providing aggregate information necessary to target resources. States may legislate conditions under which ITS information will be made available. Absent government authority, however, ITS systems should not be used as a surveillance means for enforcing traffic laws. Although individuals are concerned about public safety, persons who voluntarily participate in ITS programs or purchase ITS products have a reasonable expectation that they will not be "ambushed" by information they are providing.

6. *RELEVANT.* Intelligent Transportation Systems will only collect personal information that is relevant for ITS purposes.
ITS, respectful of the individual's interest in privacy, will only collect information that contain individual identifiers which are needed for the ITS service functions. Futhermore, ITS information systems will include protocols that call for the purging of individual identifier information that is no longer needed to meet ITS needs.

7. *SECONDARY USE.* Intelligent Transportation Systems information coupled with appropriate individual privacy protection may be used for non-ITS applications.
American consumers want information used to create economic choice and value, but also want their interest in privacy preserved. ITS information is predictive of the types of goods and services that interest consumers, for example the right location for stores, hospitals, and other facilities. However, that same information might also be used to disadvantage and harm a consumer. Therefore, the following practices should be followed.

*ITS information absent personal identifiers may be used for ITS and other purposes.
*Other unrelated uses of ITS information with personal identifiers may be permissible if individuals receive effective disclosure and have a user friendly means of opting out.
*Data collectors will only provide personal information to private organizations that agree to abide by these privacy principles.

8. *FOIA.* Federal and State Freedom of Information Act (FOIA) obligations require disclosure of information from government maintained databases. Database arrangements should balance the individuals interest in privacy and the public's right to know.
In determining whether to disclose ITS information, governments should, where possible, balance the individuals right to privacy against the preservation of the basic purpose of the Freedom of Information laws to open agency action to the light of public scrutiny. ITS travelers should be

presumed to have reasonable expectations of privacy for personal identifying information. Pursuant to the individuals interest in privacy, the public/private frameworks of organizations collecting data should be structured to resolve problems of access created by FOIA.

For further information or to submit comments please contact:
Craig Roberts
ITS America
400 Virgina Avenue, S.W., Suite 800
Washington, D.C. 20024-2730
Phone: 202/484-4847 Fax: 202/484-3483

Contact Craig Roberts at (202) 484-4847 form more information on ITS Policy and Partnerships.